Alarm Monitoring User Guide

BEST ACCESS SYSTEMS

B.A.S.I.S.® ET

BEST ACCESS SYSTEMS INTEGRATED SOLUTIONS

Table of Contents

Chapter 1: Introduction 21

Alarm Monitoring Overview 21

Conventions Used in this Documentation 21

How this Document is Organized 21

Getting Started 22

Passwords 22

Enable/Disable Strong Password Enforcement 23

Error Messages 23

Accounts 24

Log In 25

Single Sign-On Overview 26

Directory Accounts 26

Automatic and Manual Single Sign-On 27

Single Sign-On Procedures 27

Configure Single Sign-On 27

Log In Using Automatic Single Sign-On 28

Log In Using Manual Single Sign-On 29

Troubleshoot Logging In 30

Switch Log On 30

Log Out of the Application 31

Exit the Application 31

Chapter 2: Main Alarm Monitoring Window 33

Menus and Toolbars 33

Toolbar Procedures 46

How to Use the Toolbars 46

Alarm Monitoring Status Bar 46

System Administrator Procedures 47

Chapter 3: System Administrator Procedures 49

Administrative Procedures Checklist 49

Access Control Procedures Checklist 50

Monitoring Procedures Checklist 51

Video Procedures Checklist 52

Operator Procedures 53

Chapter 4: Set Alarm Monitoring Display Options 55

User-defined Display Options 55

System Status Options Window 55

Display Option Procedures 57

Select Event Types to Monitor 57

Select Column Configuration 58

Set Automatic Display Options 59

Display Multiple Windows 60

Select Hardware View Options 60

Chapter 5: Monitor Devices 61

System Status Window 61

Device Groups Window 62

Device Group Test Mode Window 64

Device Group Icons 64

Hardware Device Icons 65

Device Status 67

Procedures for Monitoring Devices 70

Update the Hardware Status 70

Perform a Device Test 70

Locate or Search for a Device 71

View the Last Connection Time for Dialup Panels 71

Download the B.A.S.I.S. Database or Firmware 72

View the Firmware Type, Flash Chip Size, and DIP Switch Settings of a Controller. 72

Chapter 6: Trace Alarms and Events 75

Trace Configuration Window 75

Procedure for Tracing 77

Trace Alarms and Events 77

Chapter 7: Video Monitoring 79

Video Monitoring Window 79

Video Player 80

Video Search Window 84

Event Settings Window 87

Video Search Performance Requirements 88

Video Monitoring Procedures 88

aLaunch Video (Live/Recorded) From a Camera 88

Load and View a Video File 89

Monitor Video in Matrix View 89
Monitor Video of Multiple Cameras (Successively) 90
Monitor Video of a Specific Camera 90
View the Video Tour 91
Set Start and End Dates 91
Export Video To A File 92
Capture an Image 92
Create a Video Event 93
Switch Camera Views Displayed in Video Player 93
Switch Between Camera and Monitor Views 93
Pan, Tilt and Zoom 93
Display the Video Search Window 95
Search Video 95
Search Specific Portions of a Camera View 96
View Search Results 98
Filter Search Results 98

Chapter 8: Video Verification 99

Video Verification Window 99
Video Verification Procedures 100
Add or Remove Readers 100
Display the Cardholder Photo and Live Video 101
Delete an Alarm in the Video Verification Window 101

Chapter 9: Control Devices and Areas 103

Grant / Deny Pop-up Window 103
Grant / Deny Pop-up Window Procedures 104
Grant or Deny Access 104

Right-click Options to Control Devices and Areas 105

General Right-click Options 105

Monitor Zone Right-click Options 106

Access Panel and Alarm Panel Right-click Options 106

Intrusion Panel and Relay Right-click Options 107

Intercom Right-click Options 107

Reader Right-click Options 107

Alarm Mask Group Right-click Options 108

Function List Right-click Options 108

Action Group Right-click Options 108

Anti-Passback Area Right-click Options 108

Guard Tour Right-click Options 109

Cisco Hardware Right-click Options 109

Single and Double Left-click Mode 109

Activate Single or Double Left-click Mode 110

Select a Device in Single or Double Left-click Mode 110

Execute a Command in Single or Double Left-click Mode 111

Chapter 10: Monitor Alarms 113

Alarm Icons 113

Pending Alarms Window 114

Procedure for Monitoring Alarms 115

Sort Alarms 115

Chapter 11: Acknowledge Alarms 117

Alarm Acknowledgment Window 117

Alarm Acknowledgment Procedures 119

Acknowledge an Alarm 120
Fast/Group Acknowledge Alarms 120
Delete an Alarm 121
Delete All Alarms 122
Display a Map 122
Example of a Map 123
View Linked Maps 123
Send an E-mail 124
Send a Page 126

Advanced Operator Procedures 127

Chapter 12: Cardholders Folder 129

Cardholders Folder Overview 129
Cardholders Folder Procedures 133
Cardholder Search Capabilities 133
Search for a Cardholder Record 135
Retrieve the Most Recent Search Results 135
Change the Cardholders Folder View Options 136
Keyboard Wedge Settings Window 137
CAC Barcodes 138
Scanning Barcodes with a Wedge Scanner 138
Keyboard Wedge Settings Window 140
Keyboard Wedge Settings Window Procedures 143
Configure a Wedge Scanner 143
Cardholder Form 144

Cardholder Form Overview 144

Cardholder Form Procedures 145

Add a Cardholder Record 145

Modify a Cardholder Record 146

Delete a Cardholder Record 146

Delete a Selected Group of Cardholder Records 146

Destroy all Cardholder Data 147

Visitor Form 147

Visitor Form Overview 147

Visitor Form Procedures 148

Add a Visitor Record 148

Modify a Visitor Record 149

Delete a Visitor Record 149

Segments Form 150

Segments Form Overview 150

Segments Form Procedures 151

Modify a Cardholder’s Segment Assignment 151

Modify a Group of Cardholder's Segments 151

Badge Form (View Mode) 153

Badge Form (Modify Mode) 153

Badge Form Procedures 157

Add a Badge Record 157

Modify a Badge Record 159

Modify Badges for a Selected Group of Cardholders 160

Encode Badge Configurations 161

Delete a Badge Record 162

Access Levels Form (View Mode) 163

Access Levels Form (Modify Mode) 163

Access Levels Form Procedures 164

Assign Access Levels to a Badge 164

Assign Activation and Deactivation Dates to Access Levels 166

Assign Access Levels to a Selected Group of Cardholders 168

Remove Access Levels From a Selected Group of Cardholders 170

Modify Access Levels Assignments 170

Delete Access Levels Assignments 170

Precision Access Form 171

Precision Access Form Procedures 172

Assign Precision Access Groups to a Badge 172

Remove Precision Access Groups From a Badge 172

Biometrics Form 173

Biometrics Form Procedures 174

Search for a Cardholder's Biometric Record 174

Visits Form (View Mode) 176

Visits Form (Modify Mode) 176

Visits Form Procedures 177

Modify a Cardholder's Permission to Have Visitors 177

Assets Form 179

Assets Form Procedures 179

Assign an Asset to a Cardholder 179

Unassign an Asset 180

Modify the Asset Group 180

Directory Accounts Form 181

Directory Accounts Form Procedures 181

Link a Cardholder to a Directory Account 181

Unlink a Directory Account 182

Guard Tours Form..... 183

Guard Tours Form Procedures 184

Assign Guard Tour Security Clearance Levels to a Cardholder 184

Reports Form 185

Reports Form Procedures 185

Run a Cardholder Report 185

Chapter 13: Badge Print Preview Window 187

Badge Print Preview Window Procedures 188

Preview and Print a Badge 188

Chapter 14: Visits Folder 191

Visits Folder Overview 191

Visit Right-Click Menu 192

Sign In Visit(s) Window 196

Print Badge(s) Window 198

Visits Folder Procedures 198

Visit Search Capabilities 199

Search for All Visits to a Selected Cardholder 199

Search for All Visits by a Selected Visitor 200

Search for Scheduled, Active or Finished Visits 201

Search for All Visits for a Specific Date or Time 202
Retrieve the Most Recent Visit Search Results 203
Find a Cardholder or Visitor Associated with a Visit 203
Add a Visit Record 203
Modify a Visit Record 208
Delete a Visit Record 208
Print a Badge for a Visitor 209
Sign in a Previously Scheduled Visit 209
Sign Out a Visit 211
Visit Form 212
Visit Form Overview 212
Select Date(s) Window 213
Select Time Range Window 214
Status Search Form 215
Status Search Form Overview 215
Details Form 217
Details Form Overview 217
E-mail Form 218
E-mail Form Overview 218
Add Recipient Window 220
Reports Form 221
Reports Form Overview 221
Reports Form Procedures 221
Run a Visit Report from the Visits Folder 221
Select Host Wizard: Search Form 224

Select Host Wizard: Search Form Overview 224

Select Host Wizard: Select Form 226

Select Host Wizard: Select Form Overview 226

Select Visitor Wizard: Search Form 227

Select Visitor Wizard: Search Form Overview 227

Select Visitor Wizard: Select or Add Form 229

Select Visitor Wizard: Select or Add Form Overview 229

Select Visitor Wizard: Add Form 231

Select Visitor Wizard: Add Form Overview 231

Select Visitor Wizard: Select Form 233

Select Visitor Wizard: Select Form Overview 233

Select Import Source Window 234

Chapter 15: Reports Folder 235

Report Configuration Form 236

Report View Filter Window 236

Report Configuration Form Procedures 240

Add a Report 240

Modify a Report 240

Delete a Report 241

Filter The Report View 241

Preview and Print a Report 241

Reader Reports Form 242

Reader Reports Form Overview 242

Reader Reports Form Procedures 246

Run a Reader Report 246

Alarm Panel Reports Form 248

Alarm Panel Reports Form Overview 248

Alarm Panel Reports Form Procedures 252

Run an Alarm Panel Report 252

Anti-Passback Reports Form 253

Anti-Passback Reports Form Overview 253

Anti-Passback Reports Form Procedures 257

Run an Anti-Passback Report 257

Date/Time Reports Form 258

Date/Time Reports Form Overview 258

Date/Time Reports Form Procedures 262

Run a Date/Time Report 262

Event Reports Form 264

Event Reports Form Overview 264

Event Reports Form Procedures 268

Run an Event Report 268

Alarm Acknowledgment Reports Form 269

Alarm Acknowledgment Reports Form Overview 269

Run an Alarm Acknowledgment Report 273

Receiver Account Zone Reports Form 274

Receiver Account Zone Reports Form Overview 274

Receiver Account Zone Reports Form Procedures 278

Run a Receiver Account Zone Report 278

Chapter 16: Assets Folder 279

Assets Form 280

Assets Form Procedures 282
Add an Asset 282
Modify an Asset 283
Delete an Asset 283
Assign a Cardholder to an Asset 284
Search for an Asset Record 284
Retrieve the Most Recent Search Results 284
Add an Asset Type/Subtype 285
Asset Classes Form (View Mode) 286
Asset Classes Form (Modify Mode) 286
Asset Classes Form Procedures 288
Assign Classes to an Asset 288
Modify an Asset Classes Assignment 288
Add Asset Groups and Classes 289
Assignments Form 290
Assignments Form Procedures 292
Assign a Cardholder to an Asset 292
Unassign an Asset 292
Search for a Cardholder Assigned to an Asset 292
Reports Form 293
Reports Form Procedures 295
Run an Asset Report 295
Chapter 17: Print Report Options Window 297
Print Report Options Window 298
Print a Report 299

Chapter 18: Report Print Preview Window 303

Report Print Preview Window 304

Report Print Preview Window Procedures 306

Preview and Print a Report 306

Search a Report for Specific Information 308

Chapter 19: Guard Tour 309

Guard Tour Overview 309

Launch a Guard Tour 309

Schedule an Automatic Guard Tour Action 313

Respond to an Automatic Guard Tour 314

View a Guard Tour 315

Checkpoint Status and Events Diagram 316

Chapter 20: Scheduler Folder 317

Scheduler Form 318

Scheduler Form Procedures 319

Add and Schedule an Action 319

Display the Scheduler Right-Click Menu 326

Add and Schedule an Action Using the Scheduler Right-Click Menu 327

Start an Action 327

Stop an Action 327

View Action History 327

View the Current Status of an Action 328

Refresh an Action 328

Refresh all Actions 329

Delete a Scheduled Action using the Scheduler Right-Click Menu 329

Modify a Scheduled Action using the Scheduler Right-Click Menu 329

Appendices 331

Appendix A: Actions 333

Actions Procedures 333

Use the Add Action Wizard 333

Action Group Properties Window 335

Action Group Properties Window Procedures 336

Add an Action Group 336

Action History/Guard Tour Event Purging Properties Window 337

Action History/Guard Tour Event Purging Properties Window Procedures 338

Add an Action History/Guard Tour Event Purging Action 338

Archive/Purge Database Properties Window 339

Archive/Purge Database Properties Window Procedures 340

Add an Archive/Purge Database Action 340

Automatic Guard Tour Properties Window 342

Automatic Guard Tour Properties Window Procedures 343

Add an Automatic Guard Tour Action 343

Change Network Video Password Properties Window 345

Change Network Video Password Properties Window Procedures 346

Schedule a One-Time Password Change 346

Schedule a Recurring Password Change 347

Deactivate Badge Properties Window 348

Deactivate Badge Properties Window Procedures 349

Add a Deactivate Badge Action 349
Device Output Properties Window 350
Device Output Properties Window Procedures 351
Add a Device Output Action 351
Device Output Group Properties Window 353
Device Output Group Properties Window Procedures 354
Add a Device Output Group Action 354
Execute Function List Properties Window 355
Execute Function List Properties Window Procedures 356
Add an Execute Function List Action 356
Global APB System/Segment Reset Properties Window 357
Global APB System/Segment Reset Properties Window Procedures 358
Add a Global APB System/Segment Reset Action 358
ISC Database Download Properties Window 358
ISC Database Download Properties Window Procedures 360
Add an ISC Database Download Action 360
ISC Firmware Download Properties Window 361
ISC Firmware Download Properties Window Procedures 362
Add an ISC Firmware Download Action 362
Mask/Unmask Alarm Input Properties Window 363
Mask/Unmask Alarm Input Properties Window Procedures 364
Add a Mask/Unmask Alarm Input Action 364
Mask/Unmask Alarm Input for Group Properties Window 365
Mask/Unmask Alarm Input for Group Properties Window Procedures 366

Add a Mask/Unmask Alarm Input For Group Action 366

Mask/Unmask Alarm Mask Group Properties Window 367

Mask/Unmask Alarm Mask Group Properties Window Procedures 368

Add a Mask/Unmask Alarm Mask Group Action 368

Mask/Unmask Door Properties Window 369

Mask/Unmask Door Properties Window Procedures 370

Add a Mask/Unmask Door Action 370

Mask/Unmask Door Forced Open Properties Window 371

Mask/Unmask Door Forced Open Properties Window Procedures 372

Add a Mask/Unmask Door Forced Open Action 372

Mask/Unmask Door Forced Open for Reader Group Properties Window .. 373

Mask/Unmask Door Forced Open for Reader Group Properties Window Procedures 374

Add a Mask/Unmask Door Forced Open for Reader Group Action 374

Mask/Unmask Door Held Open Properties Window 375

Mask/Unmask Door Held Open Properties Window Procedures 376

Add a Mask/Unmask Door Held Open Action 376

Mask/Unmask Door Held Open for Reader Group Properties Window 377

Mask/Unmask Door Held Open for Reader Group Properties Window Procedures 378

Add a Mask/Unmask Door Held Open for Reader Group Action 378

Pulse Open Door Properties Window 379

Pulse Open Door Properties Window Procedures 380

Add a Pulse Open Door Action 380

Pulse Open Door Group Properties Window 381

Pulse Open Door Group Properties Window Procedures 382

Add a Pulse Open Door Group Action 382

Reader Mode Properties Window 383

Reader Mode Properties Window Procedures 384

Add a Reader Mode Action 384

Reader Mode Group Properties Window 386

Reader Mode Group Properties Window Procedures 387

Add a Reader Mode Group Action 387

Report Print Properties Window 389

Report Print Properties Window Procedures 390

Add a Report Print Action 390

Request Print Action Flowchart 392

Reset Use Limit Properties Window 393

Reset Use Limit Properties Window Procedures 394

Add a Reset Use Limit Action 394

Sign Out Visitor Properties Window 395

Sign Out Visitor Properties Window Procedures 396

Add a Sign Out Visitor Action 396

Appendix B: Alarm/Event Descriptions 397

Appendix C: Reports 415

Index 423

Chapter 1: Introduction

Alarm Monitoring Overview

The Alarm Monitoring application displays information about individual alarms and events as they occur. Operators can acknowledge alarms and manually change the status of devices as well as monitor video and launch Guard Tours. With the correct permissions, Operators can also perform a variety of administrative tasks such as adding, modifying, deleting and tracking cardholders, visitors and assets as well as print badges.

Conventions Used in this Documentation

- Where a term is defined, the word is represented in *italics*.
- Field names, menus and menu choices are shown in **bold**.
- Keyboard keys are represented in angle brackets. For example: <Tab>.
- Keyboard key combinations are written in two ways:
  <Ctrl> + <Z> means hold down the first key and press the second

  <Alt>, <C> means press the first key, then press the second
- Window buttons on the screen are represented in square brackets. For example: [OK].

How this Document is Organized

The Alarm Monitoring User Guide is divided into three sections: the System Administrator Procedures section, the Operators section and the Advanced Operator Procedures section.

The System Administrator section outlines the steps involved in setting up an Alarm Monitoring station. Most of the procedures in these chapters reference other manuals because they cannot be performed in the Alarm Monitoring application.

The Operator Procedures section focuses on procedures to monitor alarms, monitor video, trace devices and execute commands.

The Advanced Operator Procedures section covers the administrative procedures operators can perform in Alarm Monitoring. For example, adding cardholders or visitors, printing badges, adding assets to the database and assigning assets to cardholders.

Note: Depending on the workflow of your company, some of the procedures covered in this section may be considered System Administrator procedures.

Getting Started

Passwords

B.A.S.I.S.® ET Third Edition includes strong password enforcement, which checks the user's password against password standards. This functionality is designed to enhance password security if single sign-on is not used. If single sign-on is used (automatic or manual), B.A.S.I.S. does not enforce password standards. For more information on single sign-on, refer to Single Sign-On Overview on page 26.

The system's strong password enforcement also checks the Best database user's password when logging into applications. Database user passwords apply only to Oracle and SQL databases. For information on changing your database password refer to the Installation & Setup User Guide.

Password Standards

When creating a strong password keep the following guidelines in mind:

- Passwords cannot be blank.
- Passwords cannot be the same as the user name (e.g. SA, SA).
- Passwords cannot be Best keywords (e.g. MULTIMEDIA, PROKUPETS, PROKUPET, BEST, BASIS, PASSWORD).
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (e.g. August 18, 2002).
- B.A.S.I.S. passwords are **not** case-sensitive.
- Database passwords conform to the rules of the specific database being used; passwords in SQL Server and Oracle are case insensitive.
- The maximum value for a strong password is 127 characters. The minimum value is 1.

Notes: For Oracle databases the following account username and passwords are not allowed to be used together:

System and Manager

Internal and Oracle

Sys and Change_On_Install

Enable/Disable Strong Password Enforcement

Strong password enforcement is enabled/disabled in System Administration or ID CredentialCenter. When you install B.A.S.I.S., by default strong password enforcement is enabled. When you upgrade, by default strong password enforcement is disabled. To manually enable or disable strong password enforcement:

1. Select **System Options** from the **Administration** menu.
2. Select the General System Options tab.
3. Click [Modify].
4. Select or deselect the **Enforce strong passwords** checkbox.

Note: If you disable the option to enforce strong passwords, you will continue to receive a message stating your password is weak every time you log into an application until you change your B.A.S.I.S. password to meet the password standards.

Error Messages

Read weak password messages/warnings carefully to avoid confusion about whether your user password or database password is weak.

If you have a weak database password you will receive a warning every time you log into any application, until you change your database password. Although it is not recommended, you can acknowledge the warning and continue working in the application. This table describes the password-related error messages that may be generated and which password you need to correct.

- To correct the database password, refer to the Installation & Setup User Guide.

- To correct the user password, select a password that meets the standards specified in Password Standards on page 22.

Warning message	Password to correct
Database password violations: Your password is a keyword that is not allowed. It is highly recommended that you change your password to meet our minimum password standards.	Database
Your password cannot be blank. Enter a password.	User
User password violations: Passwords cannot be the same as the user name.	User
Your password is a keyword that is not allowed.	User

Accounts

Anyone who wishes to use B.A.S.I.S. applications must enter a user name and password in order to access the software. The System Administrator should create a unique account for each user of the applications. The System Administrator can also, for each user, create a list of *permissions*, which specifies precisely which screens, fields, and buttons the user can access.

During initial installation of the application, default accounts are created. These include:

User name	Password	Type
sa	sa	system account
admin		sample
user		sample
badge		sample

These are provided as samples. You may change the passwords and use the accounts, or remove them. The exception to this is the system account, SA. By definition this account has permission to do anything in the system. A user with system access has unlimited access to the application. You cannot delete or change the system account except to modify the password, which you are strongly encouraged to do as soon as possible to discourage unauthorized use.

The first time you log into B.A.S.I.S. to configure the application, you should log in as **SA** and your password should be **SA**.

Log In

This procedure describes how to log in without using single sign-on. For a description of single sign-on, refer to Single Sign-On Overview on page 26. To log in using single sign-on, refer to Single Sign-On Procedures on page 27.

1. Click the Start button, then select **Programs** > **B.A.S.I.S. ET** > **Alarm Monitoring**.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to the next step. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. The Log On window displays.
   a. In the **User name** field, type the user name assigned to you. When logging in for the first time, your user name is **SA**.
   b. In the **Password** field, type the password assigned to you. When logging in for the first time, your password is **SA**. Note that the characters you type do not appear in the field. Instead, for each character you type, an "*" displays. This is intended to protect against unauthorized access in the event that someone else can see the screen while you type.

Important: After logging in for the first time, you are strongly encouraged to modify the password for the system account as soon as possible to discourage unauthorized use.

---

   c. In the **Directory** field, select the directory that you wish to log into. For user accounts not using single sign-on, the default is "<Internal>."
   d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.
   e. Click [OK].
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning click [Yes].
5. If you are prompted to select a monitor zone:

Monitor zone user assignments take precedence over monitoring station user assignments.

   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator

has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.

c. Select the **Save as user assignment** checkbox if you if you wish to log into the same monitor zone EVERY time you log in. This is a permanent assignment. You will not be prompted to select a monitor zone during future log ins. This is checkbox is only enabled if the user has permission.

d. Click [OK].

Note: For more information please refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:

   a. Select **No**, if you want all the queued events deleted.

   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

Single Sign-On Overview

Single sign-on simply means logging into B.A.S.I.S. with the same user name and password that you use to log into Windows or logging into B.A.S.I.S. using an LDAP user name and password for authentication. *LDAP* (Lightweight Directory Access Protocol) is a software protocol that enables you to locate businesses, people, files, and devices without knowing the domain name (network address).

Single sign-on allows scripts using the OpenIT API to authenticate. These scripts will be run under a Windows account. The account that is making the call to the API can be obtained easily this way, and the script can be restricted to those actions that the user is permitted to perform (using standard B.A.S.I.S. permissions).

Note: The use of the explicit username and password for directory authentication to Windows is strongly discouraged. It is recommended that you do not store Windows passwords in the B.A.S.I.S. system, since B.A.S.I.S. uses reversible encryption and Windows does not. If explicit authentication is required, you should use an account that has view only permission to the directory in question.

Directory Accounts

To log into B.A.S.I.S. using single sign-on, a user name, password, and directory is required. A *directory* is a database of network resources, such as printers, software applications, databases, and users. The following directories are

supported by B.A.S.I.S.: Microsoft Active Directory, Microsoft Windows NT 4 Domain, Microsoft Windows 2000/XP Workstation, and LDAP.

Automatic and Manual Single Sign-On

When a user account is configured for single sign-on, the user can log into B.A.S.I.S. automatically or manually.

For example, with automatic single sign-on, users simply start B.A.S.I.S. and they are automatically logged in under their Windows account and directory.

With manual single sign-on, users must manually enter their Windows or LDAP account information (user name and password). Users also have the option of selecting a different configured directory.

If single sign-on is not used, users manually enter a user name and a password that is different from their Windows or LDAP password. The directory is hard-coded to refer to the internal B.A.S.I.S. user directory.

Notes:

Manual single sign-on can be used with the following directories: Microsoft Active Directory, Microsoft Windows NT 4 Domain, and LDAP.

Automatic single sign-on can be used with every directory supported by B.A.S.I.S. *except* LDAP because it doesn't provide all the account information required.

Single Sign-On Procedures

Configure Single Sign-On

By default, user accounts do **not** use sign-on. To configure single sign-on the System Administrator must add a directory and link a user account to the directory.

Log In Using Automatic Single Sign-On

Automatic single sign-on is supported with Windows domain accounts.

1. Click the Start button, then select **Programs** > **B.A.S.I.S. ET** > **Alarm Monitoring**.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, “Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT.” To automatically be logged in, do nothing.
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].
5. If you are prompted to select a monitor zone:

Monitor zone user assignments take precedence over monitoring station user assignments.

   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.
   c. Select the **Save as user assignment** checkbox if you if you wish to log into the same monitor zone EVERY time you log in. This is a permanent assignment. You will not be prompted to select a monitor zone during future log ins. This is checkbox is only enabled if the user has permission.
   d. Click [OK].

Note: For more information please refer to the Monitor Zones Folder chapter in the System Administration User Guide.

---

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:
   a. Select **No**, if you want all the queued events deleted.
   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

Log In Using Manual Single Sign-On

Both users who want to log into B.A.S.I.S. using an LDAP user name and password for authentication and users who want to log in using a Windows domain account can do so using manual single sign-on.

1. Click the Start button, then select **Programs** > **B.A.S.I.S. ET** > **Alarm Monitoring**.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, "Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT."
   To manually login or to login using a different user name and password, hold down the <Shift> key. The Log On window opens.
   a. In the **Directory** field, select the directory that you wish to log into. The default is "<Internal>."
   b. In the **User name** field, type the Windows user name assigned to you. Do not enter the domain\user name just enter your user name.
   c. In the **Password** field, type the Windows password assigned to you.
   d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.
   e. Click [OK].
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].
5. If you are prompted to select a monitor zone:

Monitor zone user assignments take precedence over monitoring station user assignments.

   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.
   c. Select the **Save as user assignment** checkbox if you if you wish to log into the same monitor zone EVERY time you log in. This is a permanent assignment. You will not be prompted to select a monitor zone during

future log ins. This is checkbox is only enabled if the user has permission.

d. Click [OK].

Note: For more information please refer to the Monitor Zones Folder chapter in the System Administration User Guide.

---

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:
   a. Select **No**, if you want all the queued events deleted.
   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

Troubleshoot Logging In

If you attempted to log in and were unable to do so, make sure that the following conditions have been met:

- You entered a correct user name/password and specified the correct directory.
- If your system is configured to display an authorization warning, you accepted the terms.
- A valid license is installed. For more information refer to “The License Administration Application” appendix in the Installation & Setup User Guide.
- You have permission to use the application.
- If you attempted to log into the server and the login failed, make sure that a properly coded, licensed dongle adapter is attached to your computer’s parallel port. Make sure that your dongle is securely attached.
- If you attempted to log into a client and failed, make sure the client has a valid software license. Client computers do not need a hardware dongle attached to the computer’s parallel port. Instead, the client must have a valid software license, which is installed in the License Administration application.
- If you are using single sign-on, ensure that the directory you are authenticating against is operational and properly configured. When a directory is properly configured, the accounts are listed on the Select Account form when linking a user account to a directory.
- If you are using single sign-on, ensure that the directory account is properly linked to the user account.

Switch Log On

Switch Log On is often used when multiple operators use the same Alarm Monitoring station. Instead of logging out of the application operators can use the

switch log on feature. This simultaneously logs out the previous operator and logs in the new operator.

1. Select **Switch Log On** from the **File** menu.
2. The Log On to Alarm Monitoring window displays.
3. Enter the user name and password.
4. Select the desired directory.
5. Click [OK].

Notes: When using switch log on, the person who's logged into Windows can be a different person than the one logged into Alarm Monitoring.

Switch log on cannot be used if the new user has a monitor zone/user assignment different from the current user.

Log Out of the Application

When you log out of the application the entire application closes.

1. Select **Log Off** from the **File** menu.
2. The current user is logged off but the application remains open.

Exit the Application

You can close and exit the application using the following methods:

- Select **Exit** from the **File** menu.
- Double-click the icon located in the upper left corner of the title bar. When prompted to log off, click [Yes].

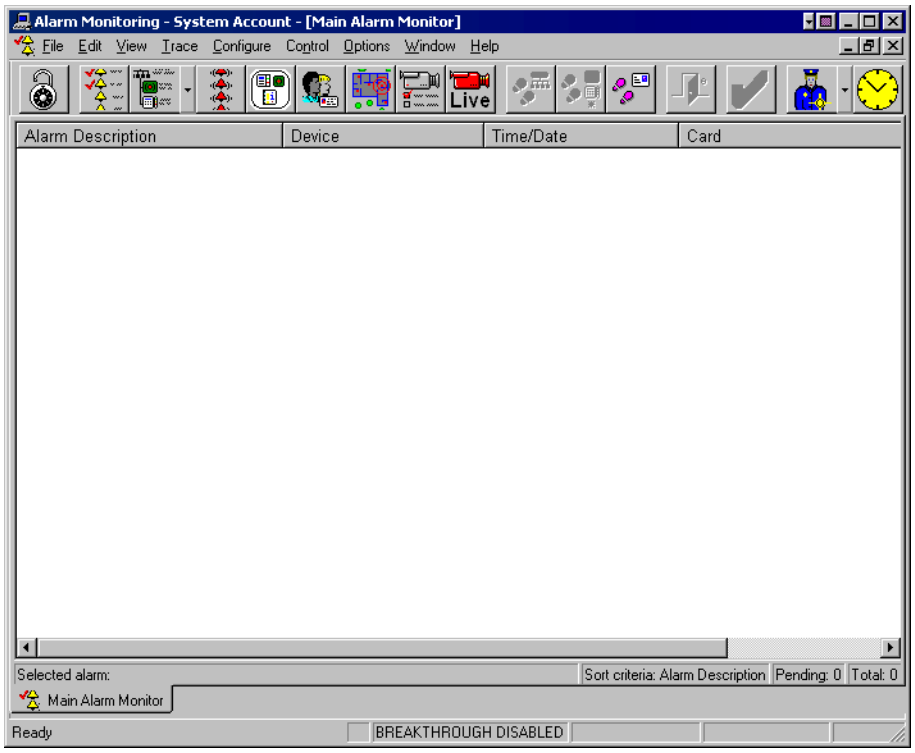
- Single click the icon located in the upper left corner of the title bar and select Close. When prompted to log off, click [Yes].

Close button

- Click the close button in the window's upper right corner. When prompted to log off, click [Yes].

Chapter 2: Main Alarm Monitoring Window

The Main Alarm Monitoring window displays automatically when you log into the application. You can open and close additional windows but the Main Alarm Monitoring window remains open until you log out of the entire application.



Menus and Toolbars

The menu bar is a horizontal list of options that appears at the top of the main window. Scroll over each option to view a drop-down menu. A toolbar is a strip of buttons positioned by default just below the menu bar. If you place your cursor over a toolbar button, a tool tip identifies the name of the toolbar button.

Operators can customize how the toolbar displays; they can:

- Change the toolbar from anchored to floating
  Toolbars are anchored by default and are displayed in horizontal rows below the menu bar. Anchored toolbars can be changed to floating toolbars, which allows the toolbar to be repositioned anywhere in the window. For more information, refer to How to Use the Toolbars on page 46.
- Control if the toolbar is displayed
  By default the toolbar is displayed. Operators can control if the toolbar is displayed by selecting or deselecting **Toolbar** from the **View** menu. For more information, refer to How to Use the Toolbars on page 46.

File menu

Menu option	Toolbar button	Function
Print		Prints information displayed in the active (topmost) window. The print toolbar button does not display if the Main Alarm Monitoring window is minimized.
Log On/Log Off		Logs you into or out of the application.
Switch Log On		Displays the login window, allowing a different user to log in without the previous user manually exiting the application. When the new user is successfully logged in, the old user is simultaneously logged out.
Change Password		Opens the Change Password dialog, enabling you to change your password (you must have the corresponding system level permission to do so).
Exit		Ends the session of every person logged on.

Edit menu

Menu option	Toolbar button	Function
Note: The following menu options are active when an alarm window is displayed.		
Acknowledge		Acknowledges the currently selected alarm.
Fast/Group Acknowledge		Allows a user to acknowledge a group of alarms simultaneously.
Delete		Removes the selected alarm from the window.
Delete All		Removes all alarms from the window.
Select All		Selects all alarms in the window.

View menu

Menu option	Toolbar button	Function
Badge Info		Displays the cardholder folder/window which contains nine forms/tabs: Cardholder, Badge, Access Level, Biometrics, Visits, Assets, Directory Accounts, Guard Tours and Reports. **Note:** When the cardholder folder/window displays, an additional menu option, **Cardholder** displays. For more information, refer to Cardholder menu on page 43.

View menu (Continued)

Menu option	Toolbar button	Function
Visits		Displays the Visits folder/window which contains the Status search, Visit, Details, Email and Reports forms/tabs. From the Visits folder/window you can: • search visit records based on scheduled time in or out and date and time the record was last changed • display visit records for a selected date range • add, modify or delete visits • print disposable badges • sign in or out a visit • send e-mail notifications • generate reports
Asset Info		Displays the Asset folder/window which contains the Assets, Assets Classes and Assignments forms/tabs.
System Status		Displays the System Status window which lists all access control devices defined in System Administration.
Device Groups		Displays the various device groups for a particular monitoring zone. Bulk operations can be performed on all parts of the device group. Types of device groups include (but are not limited to) Readers, Cameras and Input and Output groups.
Pending Alarms		Displays the Pending Alarms window. To return to the Main Alarm Monitoring window click the View Alarms toolbar button.
Video Verification		Launches the Video Verification window where you can compare live video to a cardholder's photograph.
Video Monitoring		Launches the Live Video window which is used to run a video tour of the cameras defined in Camera Groups.

View menu (Continued)

Menu option	Toolbar button	Function
Map		Displays a map containing the device associated with the selected alarm (if the Main Alarm Monitoring window is active) or the selected device (if the System Status window is active). • If the selected device is represented on more than one map you will be prompted to select the map of choice. • A message displays if the selected device is not represented on any map. • To display the **View Map** menu option, right-click a device in the System Status window or select an alarm in the Main Alarm Monitoring window.
Default Map		Displays the map that is assigned to that monitoring zone. This menu option is dimmed if no map has been assigned to this zone.
Map Selection		Displays a window in which all available maps are listed. This menu option is dimmed if no maps are available.
Scheduler		Displays the Scheduler window which is used to add, modify and delete scheduled actions within the B.A.S.I.S. system. An *action* is any task that can be performed by software as a result of an event of schedule, for example; download a database, mask/unmask alarm inputs, pulse open a door and reset the use limit. **Note:** The Scheduler window is also available by selecting **Administration** > **Scheduler** in System Administration. For more information, refer to the Scheduler Folder chapter in the System Administration User Guide.
Reports		Displays the Reports folder/window of data entry forms/tabs.
Sort by		Sorts alarms according to criteria chosen in the submenu.
Toolbar		Displays the toolbar when selected (checked).
Status Bar		Displays the status bar when selected (checked).

Trace menu

Menu option	Toolbar button	Function
Monitor Zone		Monitors or traces alarms for the selected monitor zone.

Trace menu (Continued)

Menu option	Toolbar button	Function
Controller		Monitors or traces alarms for the selected access panel/controller. An access panel/controller is a device that acts as the focal point for a group of card readers. The **Controller** menu option or toolbar button becomes active (not grayed out) when you highlight an access panel/controller or any device under a given access panel/controller in the System Status window. **Note:** Access panel/controller traces are recursive, meaning all events occurring on that access panel/controller are included.
Device		Monitors or traces alarms for the selected device. The **Device** menu option becomes active (not grayed out) when you highlight a device in the System Status window. **Note:** This menu option can be used to trace all device types including alarm outputs, reader aux inputs and reader aux outputs.
Badge		Monitors or traces alarms for a specific badge.
Asset		Monitors or traces alarms for the selected asset. The **Asset** menu option becomes active (not grayed out) when you highlight a device in the System Status window.
Area		Monitors or traces alarms for the selected intrusion area. The **Area** menu option becomes active (not grayed out) when you highlight a device in the System Status window.

Configure menu

Menu option	Function
Alarm Filter	Displays a checklist of alarm types to monitor. The **Alarm Filter** menu option becomes active (not grayed out) when you display an alarm window.
Columns	Displays a list of columns from which to display. The **Columns** menu option becomes active (not grayed out) whey you display an alarm window.
Hardware Status Frequency	Determines how often background updates are performed. The choices are “No Updates”, 10, 15, 20, 30 and 60 minute intervals. This is saved per user / per station and only applies to Apollo hardware.
System Status Options	Displays the System Status Options window which is used to specify how the System Status window displays information and what devices are included.

Control menu

Menu option	Toolbar button	Function
Update All Hardware Status		Updates the status of all access panels in the monitoring zone.
Set All Controller Clocks		Sets the clocks in all access panels according to the machine on which the driver is running.
"Current Device"		This menu option is dynamic, meaning the name of this menu option changes according to the device highlighted in the System Status window. For example if a BAS-1300 HID reader is highlighted in the System Status window, then BAS-1300 HID displays in the Control menu options. Each "Current Device" menu option also has sub-menu options. A separate table exists for these sub-menu options on page 38.
Guard Tour		Allows Operators to launch or view a guard tour. Guard tour provides a guard (a cardholder who has been specifically chosen to conduct a tour) with a defined set of tasks that must be performed within a specified period of time. Typical tasks include swiping a card at a checkpoint access reader or turning a key connected to an alarm panel input. To use guard tour the Linkage Server must be properly configured. For more information, refer to the System Options Folder chapter in the System Administration or ID CredentialCenter User Guide.

Control menu - "Current Device" sub-menu

Sub-menu option	Toolbar button	Function
Note: The "Current Device" sub-menu options that are available depend on the type of device listed as the "Current Device" in the **Control** menu. The type of device listed as the "Current Device" in the **Control** menu depends on the device highlighted in the System Status window.		
Current Status		Displays current status of device.
Acknowledge		Acknowledges the selected alarm.
Trace		Traces the selected device.
Update Hardware Status		Polls currently selected access panel/controller and updates the hardware status. If a downstream device (like a reader) is selected, the update hardware status is done for the controller associated with that device.
Properties		Displays access panel/controller properties.
Open Door(s)		Pulses open any door associated with selected access panel/controller or reader. To activate the Open Door(s) toolbar button you must select an access panel/ controller or reader, otherwise the option is grayed out.
Set Controller Clock		Sets selected access panel/controller clock to current time. If a device other than an access panel/controller is selected, this option sets the clock on the access panel/controller to which the device is attached.

Control menu - "Current Device" sub-menu (Continued)

Sub-menu option	Toolbar button	Function
Reader Access Modes		Updates the reader mode of every reader associated with selected access panel/ controller or reader.
Reader Biometric Verify Mode		Enables/disables verify mode for access control readers with an associated biometric reader. • When verify mode is enabled, the normal card and/or pin access is and a biometric match is required. • When verify mode is disabled, only the card and/or pin access is required.
Reader First Card Unlock Mode		Enables/disables the Reader First Card Unlock Mode. The Reader First Card Unlock Mode is a qualifier for online Reader Mode. When enabled, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked. Whenever a Reader enters or leaves First Card Unlock Mode, an event transaction is logged in the database and displayed in Alarm Monitoring. **Note:** The Reader First Card Unlock Mode can also be enabled/ disabled via the Reader folder/window in System Administration, via local timezone control in the BAS-2000 and as part of the Reader Mode or Reader Group Mode action used in the Scheduler and Global I/O. **Note:** Reader First Card Unlock Mode is only supported on the BAS-2000 controller. However, first style unlock behavior can be configured for use with any access controller through Best's Global I/O Support.
Activate		Activates the selected alarm output.
Deactivate		Deactivates the selected alarm output.
Pulse		Pulses an output device.
Mask		Masks an input device. The System Status window displays `masked` beside the selected device.
UnMask		Unmasks an input device.
Receiver account information		A *receiver* is a piece of hardware used to receive events from multiple accounts in multiple formats. Downstream devices connect to receivers via phone lines, direct wire connections and LAN connections. The receive account information displays information about a specific receiver.
View Map		Displays a map associated with the selected device (if one exists). If more than one map exists, the user is prompted to select a map.
Launch Video		Displays video for the selected device if a camera is associated with the device.

Control menu - "Current Device" sub-menu (Continued)

Sub-menu option	Toolbar button	Function
Download Firmware		Downloads firmware to the following downstream devices: Dual Interface Rdr1 readers, BAS-1100 and BAS-1200 alarm panels, and RS-485 command keypads. **Note:** It is not possible to download firmware to a single reader interface.
Download Database		Downloads the database to the access panel/controller.
Reset Use Limit		Resets the number of times a badge can be used on a particular access panel/ controller.
Connect		Connects the access panel/controller via a dialup/modem connection.
Disconnect		Disconnects the access panel/controller via a dialup/modem connection.
Execute Custom Function		Executes a custom function associated with the Radionics Intrusion Controller. This menu option is only available with Radionics Intrusion Controllers.

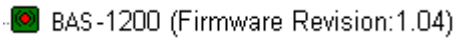
Options menu

Menu option	Function
Mute Sound	Disables the audio portion of the system when selected (checked).
Font	Selects the font used in Alarm Monitoring.
Save Alarms on Exit	Saves all currently displayed alarms at the end of a session,when selected (checked).
Save Settings on Exit	Saves screen characteristics at the end of a session, when selected (checked).
Save Settings Now	Saves screen characteristics immediately.
Ascending Time/ Date	Lists alarms in ascending order of time and date (i.e., oldest first), when selected (checked).
Descending Time/ Date	Lists alarms in descending order of time and date (i.e., newest first), when selected (checked).
Display Seconds	Includes seconds in the displayed alarm times, when selected (checked).
Auto Cardholder Display for Access Alarms	Displays the cardholder associated with an incoming alarm whenever the alarm deals with a badge id. • If selected (checked), Alarm Monitoring displays the cardholder associated with access alarms. • If not selected (unchecked), Alarm Monitoring does NOT display the cardholder associated with access alarms.

Options menu (Continued)

Menu option	Function
Automatic Map Display	Automatically displays a map when the alarm arrives, if selected (checked) and if the associated device exists on a map. If the device exists on multiple maps, the first one found will be displayed. This feature must also be configured in System Administration **Monitoring** > **Alarms** menu, Alarm Definitions tab/form.
Automatic Cardholder Display	Applies to alarms for which the **Show Card Holder** check box is selected in the System Administration software. To locate this checkbox select the **Monitoring** menu and then select **Alarms**. Click the Alarm Definition tab. • If selected (checked), the corresponding cardholder view automatically displays when the alarm arrives if the alarm is related to a badge id. • If the cardholder view is already displayed when a new alarm arrives, the new cardholder associated with the alarm is searched for and displayed. • If not selected (unchecked), the corresponding cardholder view does not automatically display when an alarm occurs.
Automatic Video Verification	Applies to alarms for which the **Video Verification** check box is selected in the System Administration software. To locate this checkbox select the **Monitoring** menu and then select **Alarms**. Click the Alarm Definition tab. • If selected (checked), the corresponding video verify view automatically displays when the alarm occurs. • If not selected (unchecked), the corresponding video verify view does not automatically display when the alarm occurs.
Automatic Visual Notification	Causes breakthrough alarms to occur. By default, this menu choice is selected (checked) in Alarm Monitoring. • If selected (checked), breakthrough alarms cause the Monitoring application and the Main Alarm View to be brought to the foreground when an alarm occurs. • If not selected (unchecked), breakthrough alarms occur in the background. Automatic visual notification must be configured for individual alarms in System Administration. From the **Monitoring** menu select **Alarms**. Click the Alarm Definition tab. Highlight the appropriate alarm, click the [Modify] button, select the **Visual Notification** checkbox. Click the [OK] button. In the Alarm Monitoring application be sure to refresh the Alarm configuration through the **Options** menu.
Automatic Live Video Display	Displays live video automatically when an alarm occurs, if selected (checked).
Display Status On Maps	Displays the status of all device icons on graphical maps. • If selected (checked), the status of every device icon on a graphical map is displayed (e.g. reader mode, online/offline, occupancy number). • If not selected (unchecked), the status will only be displayed for a given device as a tool tip when the mouse pointer is over the device icon.

Options menu (Continued)

Menu option	Function
Highlight Entire Row	Highlights the entire row of an alarm when selected (checked).
Disable Command Verification	Displays "successful configuration" messages when commands to hardware, E-mail and pages are successfully sent. • If selected (checked), Alarm Monitoring will NOT display "successful configuration" messages. • If not selected (unchecked), Alarm Monitoring displays "successful configuration" messages. Errors display in message boxes regardless of this setting.
Execute Command on Single Click of Icon	Specifies commands to be executed on a single click. This setting may be configured for each user and saved along with other user settings. • If selected (checked), then a single click executes the default command for the device configured in System Administration. • If not selected (unchecked), then the default command executes on a double-click.
Display Controller Capacity	Displays available memory, free memory, the maximum number of cardholders, current cardholders stored in a controller, maximum number of biometric templates and the current number of biometric templates set in a controller. This information is displayed in the System Status window and is mainly used for diagnostic purposes. By default, this option is unchecked. • If selected (checked), the controller capacity information displays. • If not selected (unchecked), the controller capacity information is NOT displayed.
Display Device Firmware Versions	Displays firmware version (major and minor) for downstream devices. The minor firmware version number displays as the last two digits. The firmware version of controllers and gateways display regardless of this option.  **Note:** The firmware version is that of the interface board. • If selected (checked), the current firmware version displays for devices including single interface readers, dual interface Rdr1 readers, BAS-1100 and BAS-1200 alarm panels, cameras and RS-485 command keypads. • If not selected (unchecked), the firmware version displays as part of the status when the mouse pointer is over the device icon. However the firmware version of controllers and gateways always displays, regardless of this option.
Refresh Alarm Configuration	Causes alarm configuration information to be refreshed.

Window menu

Menu option	Function
Cascade	Places all open windows in an overlapping arrangement with the active window displayed on top.
Tile Horizontally	Places all open windows in a horizontal, non-overlapping arrangement.
Tile Vertically	Places all open windows in a vertical, non-overlapping arrangement.
Arrange Icons	Places all minimized windows (title icons) in a row.
Close “options”	There are several menu options to close different windows in the Alarm Monitoring application (e.g. Close Badge Info, Close Visits).
Numbered choices	Lists all open windows. The active (topmost) window is indicated by a checkmark.

Help menu

Menu option	Function
Contents	Displays online help for the currently displayed window.
Index	Displays the online help table of contents.
About Alarm Monitoring	Displays version and copyright information.

Cardholder menu

Menu option	Function
Note: This menu is only available after you select **View** > **Badge Info** from the menu options.	
Show Unassigned Assets	If selected, both assets that currently are and assets that once were (but have since been unassigned) assigned to the selected cardholder will be displayed in the listing window on the Assets form. If not selected, only assets that are currently assigned to the selected cardholder will be displayed.
MobileVerify	When selected, displays the MobileVerify Options window where the gate assigned to the current MobileVerify workstation can be changed, or the system’s Force Protection Setting can be overridden. For this option to be available, the following conditions must be met: • The user must have the MobileVerify Workstation Options permission, which is set on the MobileVerify sub-tab of the System Permission Groups form in the Users folder. • A recommendation label must have been added to the Cardholder form using FormsDesigner. (The recommendation label may be on a new separate tab or on the Cardholder form.) • The current workstation must have a gate configuration assigned to it. This is done on the Gate Configuration sub-tab of the Workstations form in the Workstations folder.

Cardholder menu (Continued)

Menu option	Function
Keyboard Wedge Settings	When selected, displays the Wedge Scanner Settings window where you can configure how the B.A.S.I.S. system interprets the information it receives from a wedge reader. You must have administrative rights to the workstation when setting these options. These settings are set per workstation.
View Options	When selected, displays the View Options window from where you can choose cardholder search attributes.
One Free Pass	If selected, allows the selected cardholder to violate anti-passback rules one time.
APB Move Badge	When selected, displays the Area Move Badges window from where you can move a badge to a new area.
Display Global APB Areas	When selected, displays the Cardholder Global Anti Pass Back (APB) Areas window. This window lists the global APB areas that the selected cardholder is currently located in.
Show Last Granted Location	If selected, the **Last access** field will display information about the most recent valid access by the selected cardholder, including the triggered event, date, time and reader name.
Show Last Attempted Location	If selected, the **Last access** field will display information about the most recent access attempt (whether access was granted or not) by the selected cardholder, including the triggered event, date, time and reader name.
Bulk	Provides a sub-menu of options that can be applied to a select group of cardholder records.
First Record	Displays the first matching cardholder record.
Rewind	Jumps back 10 matching cardholder records.
Previous Record	Displays the previous matching cardholder record.
Next Record	Displays the next matching cardholder record.
Fast Forward	Jumps forward 10 matching cardholder records.
Last Record	Displays the last matching cardholder record.

Cardholder menu - Bulk sub-menu

Menu option	Function
Note: The **Bulk** sub-menu is only available when the **Cardholder** menu is available. **Note:** The **Bulk** sub-menu options are available when a cardholder record is displayed in the Cardholders folder/window.	
Assign Access Levels	Allows you to assign access levels to a select group of cardholder records.
Remove Access Levels	Allows you to remove access levels from a select group of cardholder records.
Modify Badges	If selected, displays the Bulk Modify Badges window from where you can choose to update one or more of the following fields in the Cardholders folder/window: **Activate Date**, **Deactivate Date**, **Badge Status** and **Use Limit**. You can apply a filter as to which badges you want to update, based on status and/or type. Note that when updating the **Badge Status** field, you must select a badge status filter.

Cardholder menu - Bulk sub-menu (Continued)

Menu option	Function
Change Cardholder Segments	When selected, the Bulk Segment Change window opens from where you can change a selected group of cardholder record's segment assignment.
Change Cardholder Replication	When selected, the Change Cardholder Replication window opens from where you can select a new replication setting. **Note:** This menu option applies only to Enterprise systems.
Delete Cardholders in Search	Allows you to delete cardholders to a select group of records.
Destroy ALL Cardholder Data	Allows you to destroy all cardholder data.
View Log	Displays the Log Viewer window from where you can view a log of bulk events.

Asset menu

Menu option	Function
Note: This menu is only available after you select **View** > **Asset Info** from the menu options.	
First Record	Displays the first matching asset record.
Rewind	Jumps back 10 matching asset records.
Previous Record	Displays the previous matching asset record.
Next Record	Displays the next matching asset record.
Fast Forward	Jumps forward 10 matching asset records.
Last Record	Displays the last matching asset record.
Asset Groups and Classes	Displays the Asset Groups and Classes Management folder/window.
Asset Types and Subtypes	Displays the Asset Types and Subtypes Management folder/window.
Show Assignments X Days Past	Displays the Filter Out Assignments After X Days window, which allows you to specify the number of days you want to view.
Bulk Add Mode	Enables you to quickly enter multiple Scan IDs for the same type of asset (e.g. enter multiple Scan ID's for 10 portable PCs). To display the **Bulk Add Mode** menu option an asset record must be open in the Assets folder/window.

Toolbar Procedures

How to Use the Toolbars

Alarm Monitoring utilizes one standard Windows toolbar.

If you want to:	Procedure:
Display the name of a toolbar button	Point to the toolbar button with the mouse (without clicking).
Use a toolbar button to perform a command or function	Click the toolbar button with the left mouse button.
Change the toolbar from "anchored" to "floating" Change the toolbar from "floating" to "anchored"	Double-click an empty area of the toolbar.
Hide or display the toolbar	From the **View** menu select **Toolbar**. A checkmark appears next to the toolbar if it is not hidden. Toggle the toolbar to display or hide.

Alarm Monitoring Status Bar

The Alarm Monitoring status bar, located in the lower portion of the screen provides different information, depending on what window is displayed.

Main Alarm Monitoring Window Status Bar

The Main Alarm Monitoring window displays the following information in the status bar:

- **Selected alarm:** the name of the selected alarm, if any. If multiple alarms are selected simultaneously, the last one that was selected is indicated here.
- **Sort criteria:** the information by which the list of alarms is currently sorted.
- **Pending:** the number of alarms that are currently pending. Pending alarms include all existing normal or initiating alarms marked as "Active" that are still displayed in the main alarm view and have not been acknowledged.
- **Total:** the total number of alarms currently in the window.
- **Verified mode enabled:** an access control reader that has an associated biometric reader, is in verify mode.

Note: For information about the status bar information provided in the System Status window refer to the table on page 62.

System Administrator Procedures

Chapter 3: System Administrator Procedures

The Alarm Monitoring application is not only designed to monitor alarms and events, but it can also be used for a variety of administrative tasks such as adding cardholders or visitors, printing badges, adding assets to the database and assigning assets to cardholders. Depending on how the System Administrator sets the cardholder and system permissions, users with access to Alarm Monitoring can add, modify and delete cardholder, badge and asset information as well as capture images and perform bulk operations.

This chapter assumes that an Alarm Monitoring Station has been physically set up and focuses on the procedures the System Administrator should complete to enable procedures to be performed by Alarm Monitoring Operators. Refer to the B.A.S.I.S. disks to determine the PC requirements for an Alarm Monitoring Station (client or server) and refer to the Installation and Set Up User Manual for physically setting up the hardware.

Note: Additional System Administrator procedures may be included in the Advanced Operator Procedures section starting on page 127.

Administrative Procedures Checklist

The administrative procedures are completed via the **Administration** menu in the System Administration application. Instructions can be found in the Administration section of the System Administrator User Guide.

- **Create card formats** - card formats (asset, magnetic, smart card, etc.) are required to configure a reader
- **Create badge types** - (employee, visitor, etc.)
  - printing/encoding badge options
  - required cardholder fields
  - badge ID allocation for generating ID numbers
  - guest defaults (extended strike/held times, passage mode, deadbolt override)
- **Add directories** - required for single sign-on
- **Set system, cardholder, monitor and field/page permissions**
- **Add users**
  - user name
  - internal account and password
  - directory account
  - segment access
  - area access manager levels
- **Add Alarm Monitoring workstations** - workstations are required to configure hardware devices
  - add dot matrix printer via workstations folder

  - connect a printer locally (directly to the Alarm Monitoring workstation).

- **Set general system options**
  - log on authorization warning
  - strong password enforcement
  - number of days to save queued events
  - linkage server host
  - OpenIT service
  - DataExchange server host
  - KnoWho server

- **Set cardholder options and visits**
  - maximum number of badges per cardholder
  - ability to create/save photo thumbnails
  - badge PIN types (4, 6 or 9-digits)
  - PIN code generated (random or manual)

Precision access mode determines the readers that cardholders have access to.

  - precision access mode
  - use or lose badge feature (change badge status to lost or returned after a specified amount of time)
  - visits options
  - cardholder, visitor and visit search result options

- **Configure global output devices**
  - SMTP server settings to use when sending e-mail
  - GOS paging device
  - recipients of e-mail and page messages

- **Configure e-mail and paging notification**
  - fields and display order for e-mails and paging
  - fields and/or directories to check when determining who to send an e-mail notification to

- **Add segments to your installation**
  - enable segmentation
  - segment options

List options are created using list builder.

- **Create list options**

- **Set up archiving parameters**

Access Control Procedures Checklist

This portion of the chapter focuses on the procedures the System Administrator should complete to enable access control and monitoring procedures to be performed by Alarm Monitoring Operators.

Note: Be sure to complete the administrative procedures listed at the beginning of this chapter before attempting any access control and monitoring procedures. Several access control and monitoring procedures require that certain

administrative procedures be completed first. For example you must configure a workstation before you can configure most hardware devices.

All System Administrator access control procedures are completed via the **Access Control** or **Additional Hardware** menu in the System Administration application. Instructions can be found in the Access Control section of the System Administration User Guide, chapters 25 through 36 as well as the Additional Hardware section, chapters 42 through 46. A separate Intrusion Detection User Guide also exists if you are going to configure intrusion detection devices.

- **Configure hardware devices**
  - dialup modem
  - access panels
  - readers
  - alarm panels
- **Additional access control configurations**
  - timezones (specify holidays, assign readers and modes of operation)
  - access levels
  - anti-passback areas (normal, safe and hazardous areas for mustering)
  - alarm mask groups (un/mask multiple alarm inputs simultaneously)
  - device groups (input/output readers)
  - local and/or global inputs and outputs
- **Configure additional hardware**
  - fire panels
  - intercom devices
  - personal safety devices
  - receivers
  - intrusion detection devices

Monitoring Procedures Checklist

System Administrator monitoring procedures are completed via the **Monitoring** menu in the System Administration application. Instructions can be found in the Monitoring sections of the System Administration User Guide, chapters 37 through 39.

- **Customize alarms, instructions, acknowledgment notes and acknowledgment actions**

Alarm mask groups enable you to un/mask multiple alarm inputs and readers simultaneously.

  - alarm mask groups
  - customize and configure alarms
  - text instructions
  - audio
  - acknowledgment notes
  - automatic acknowledgment actions
- **Configure monitor zones**
  - event routing group

  - monitor zones
  - monitoring station assignments

- **Set up guard tours**
  - checkpoint actions
  - messages and checkpoint events
  - monitoring stations
  - link camera devices to the checkpoints
  - special instructions

- **Set Monitoring Options**
  - associate a command with a device or area icon (enables operators to execute a command with a single and double left-click in the system status tree and map view)

- **Create Alarm Monitoring Maps**

Video Procedures Checklist

All the video procedures are completed via the **Video** menu in the System Administration application. Instructions can be found in the Video section of the System Administration User Guide, chapters 40 and 41.

- **Configure video**
  - matrix switcher
  - video devices (recorders and cameras)
  - link hardware devices to a camera
  - alarm-video configurations
  - add a video recorder to a monitoring zone

- **Configure video verification**
  - CCTV Controller associated with a workstation
  - CCTV Command (located on **Access Control** > **Readers** > Control tab)

Operator Procedures

Chapter 4: Set Alarm Monitoring Display Options

User-defined Display Options

Several windows in Alarm Monitoring can be configured to display according to user preference. These views are recreated every time the user logs into the application.

The following is a list of user-defined display options that are set from the **Configure** or **Options** menu.

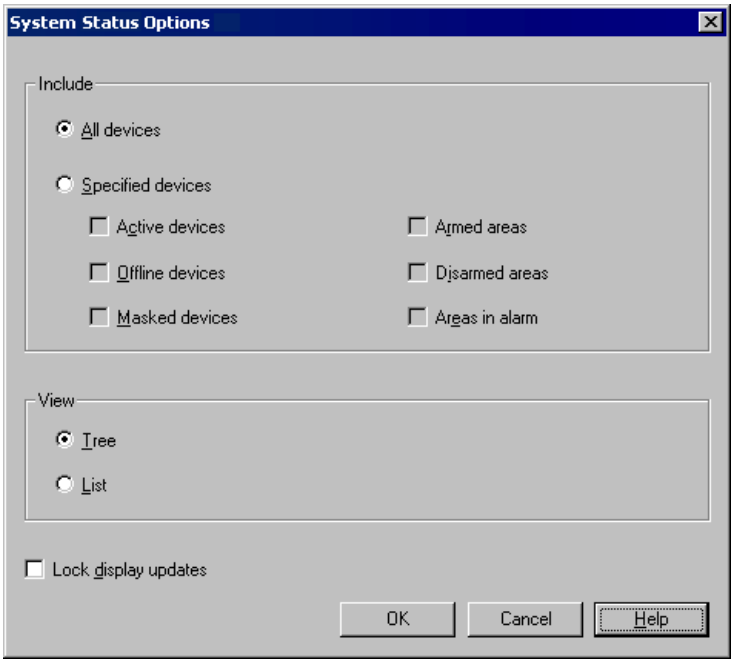
- Select Event Types to Monitor
- Select Column Configuration
- Set Automatic Display Options
- Select Hardware View Options

Note: The Select Hardware View procedure displays the System Status Options Window.

System Status Options Window

The System Status Options window is displayed from the System Status window. Verify you are in the System Status window, then select **Configure** > **System Status Options** from the menu.

You can also display the System Status Options window by clicking the System Status icon that displays to the left of the **File** menu (when you open the System Status window).



Button/field	Description
All devices	Displays all the devices (active, offline, masked, armed, disarmed and areas in alarm) in the System Status window.
Specified devices	Displays specific types of devices including: **Active devices** Displays only active devices in the System Status window. **Offline devices** Displays only offline devices in the System Status window. **Masked devices** Displays only masked devices in the System Status window. **Armed areas** Displays only armed areas in the System Status window. An *area* is a separately configured section of an Intrusion Detection Panel, sometimes referred to as a *partition*. To arm an area means to "turn on" the protection for an area. **Disarmed areas** Displays only disarmed areas in the System Status window. **Areas in alarm** Displays only areas that have an active alarm triggered. **Note:** If one or more of the specified device selections are made; only devices matching those criteria display in the view.

Button/field	Description
View	Displays information about devices in one of two formats: **Tree** Displays information in a hierarchical fashion, also called a tree or branching arrangement. Each entry in the list represents one device. Panels have the leftmost entries and any device connected to a panel is listed below the panel and indented to the right. **List** Lists the following information about devices in the system: • Device (Name) • Parent Device (Name) • Current Device Status **Note:** The hardware list displays separate rows for Reader Auxiliary Input and Reader Auxiliary Output devices.
Lock display updates	Prevents items from being added or deleted from the display window. When the **Lock display updates** checkbox is selected an indicator on the status bar displays "LOCKED." Devices cannot be added to or deleted from the display window. The status of devices currently in the window update as their status changes. The if the status of devices not in the window change they are not added to the display window. When the **Lock display updates** checkbox is not selected the status bar indicator is blank. Devices are added to and removed from the display window automatically as their device status changes. For example, if an input becomes active and the view is displaying active devices, the input will be added to the view. If the input is now restored, it will be removed from the view.
OK	Accepts the settings and closes the window.
Cancel	Closes the window without saving any changes made to the settings.
Help	Displays help for this topic.

Display Option Procedures

Select Event Types to Monitor

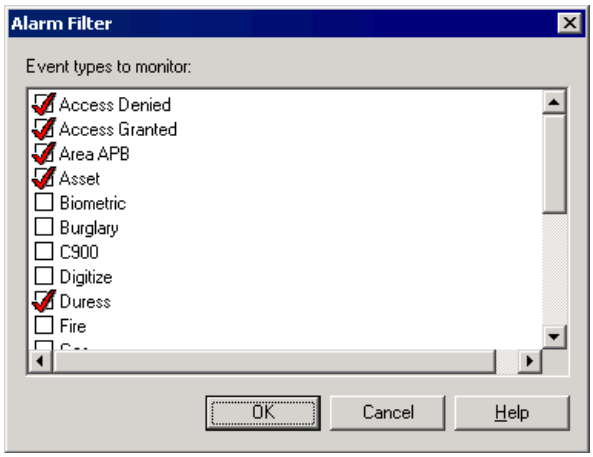
If you have permission to edit alarm filters, you can apply an alarm filter to each view in Alarm Monitoring, including the main alarm view, pending alarm view, video verification view and any trace view. Each of theses views can be

configured to filter out alarms independent of each other, however, only the main alarm view filter is saved from session to session.

The alarm filter determines which alarms display based on the type of event the alarm is associated with.

For example, you may wish to display every alarm for a specific reader's trace window but you may not wish to display "Access Granted" alarms in the Main Alarm Monitoring window. You can apply both of these filters to the different views, but when the session ends, only the filters applied the main window are saved.

1. Open the window from which you want to select the events displayed. Verify this window is the active (topmost) window.
2. From the **Configure** menu select **Alarm Filter**. The Alarm Filter window displays.



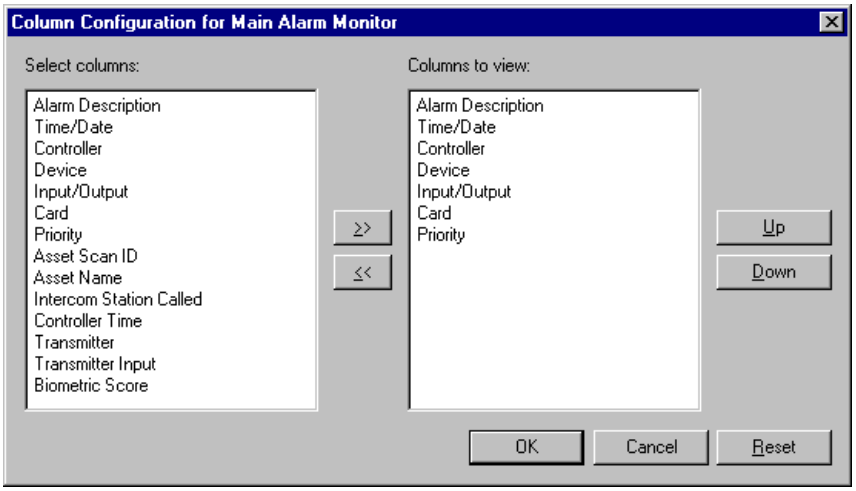
3. By default, all event types are selected (have a checkmark). If you do not want to display a particular category of events, click that option to deselect it (remove the checkmark). Click the option again to select it.
4. Click [OK] to close the Alarm Filter window

Select Column Configuration

You can rearrange the order of the columns in any window as well as add or remove columns that display. This is done independently for each type of window. For example, if the column configuration is changed for an alarm window, this becomes the default for all alarm windows of the same type. If the

column configuration is changed for a given reader trace, this will become the default configuration for all reader traces.

1. Open the window from which you want to configure the columns displayed. Verify this window is the active (topmost) window.
2. From the **Configure** menu select **Columns**. The Column Configuration window displays.



3. In the **Select columns** display field, click/highlight the name of a column, then click [>>]. The column name appears in the **Columns to view** display field.
4. Arrange the column names in the order you want them to appear.
   - Click/highlight a column name in the **Columns to view** display box. Then use the [Up] and [Down] buttons to change the column's relative position.

Note: The order the column names appear in the **Columns to view** display field is the same order the columns will display in the window which you are configuring the columns for.

5. Click [OK] and the window displays the new column configuration.

Set Automatic Display Options

Several display options are available from the **Options** menu. To activate an option select it (place a checkmark beside it). To deactivate an option select it again to remove the checkmark. For information on the options available from the Options menu.

Display Multiple Windows

1. Open the desired windows using the toolbar buttons or menu options.
2. From the **Window** menu select one of the following:
   - Cascade
   - Tile Horizontally
   - Tile Vertically
3. Using the mouse, click and drag each window to resize and relocate it.

Select Hardware View Options

Hardware view options include list or tree view as well as the type of devices displayed. Users can display every device or select devices that meet a specific criteria such as active, offline and/or masked devices as well as armed areas, disarmed areas and/or areas in alarm.

1. Verify you are in the System Status window, then select **Configure** > **System Status Options** from the menu.
2. The System Status Options window displays.
   a. Select the type of device you would like to display by clicking either the **All devices** or **Specified devices** checkbox. If you selected the **Specified devices** checkbox, select the desired device by clicking the appropriate radio button (active, offline or masked devices).
   b. Select the **Tree** radio button to view the system hardware in a tree or branching format.
   c. Select the **List** radio button to view a list of devices, their current status and parent device.
   d. Select the **Lock display updates** checkbox if desired.
3. Click [OK].

Chapter 5: Monitor Devices

The System Status window and Device Groups window are used to monitor devices.

System Status Window

The System Status window lists every access control device, area or action group defined in System Administration for a specific segment. Other configuration settings are listed in parenthesis after each device.

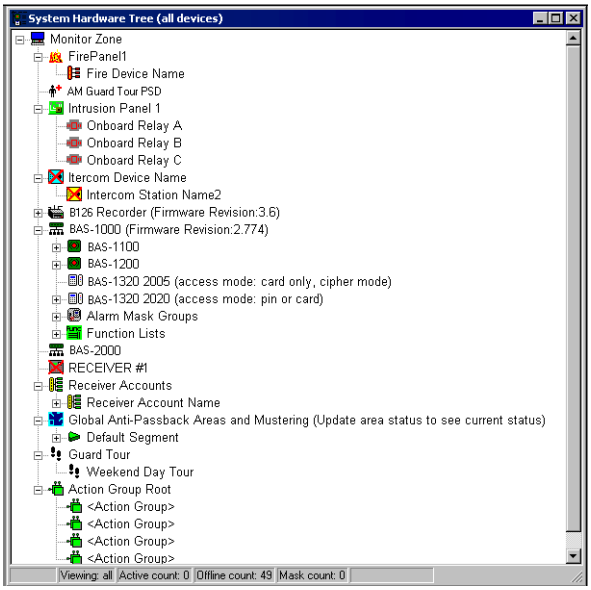
Displayed by:

The System Status window can be displayed several ways:

- Click the triangle on the System Status button and select an existing window or open a new one.

Note: Clicking the System Status button (not the triangle) brings up a new System Status window if there is none present. If a System Status window is already open, clicking the System Status button causes the default (first) window to display.

- From the **View** menu, select **System Status** and then the window you want to display.
- Choose one of the numbered options under the **Window** menu.
  - Though rare, if more than nine System Status windows are open, the **More Windows** menu option will be available. Choose a window from the list and click [OK] to bring it to the foreground.



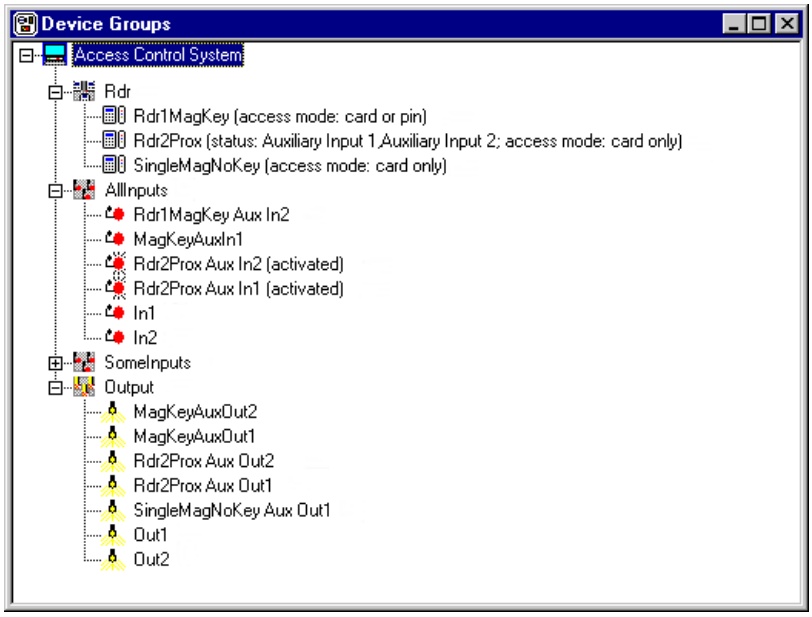
Field	Description
Display window	The information in the window is displayed in hierarchical fashion, also called a tree or branching arrangement. Each entry in the list contains the name of one device. Access Panels have the leftmost entries. For a specific Access Panel, a device connected to it is listed below and indented to the right. Each device connected to those devices is listed below them and further indented. An icon to the left of each entry identifies the entry's type.
Hardware Status Bar	Located on the lower right portion of the screen, the status bar on the System Status window has four counters: **Viewing:** Shows the number of devices viewed. **Active count:** Shows the number of active points in the monitoring zone. This is NOT the same as the number of active devices. For example, if a reader is in the Door Forced Open, Door Held Open and Reader Tamper states, the active count is increased by three. The active device number is not increased. **Offline count:** Shows the number of offline devices in the Monitoring Zone. Every device is counted including alarm inputs, reader auxiliary inputs, alarm outputs and reader auxiliary outputs. **Masked count:** Shows the number of masked points in the monitoring zone. **MUSTER MODE:** This portion of the status bar only displays when a Monitoring Zone is in Muster mode.

Device Groups Window

The Device Groups window displays the currently configured device groups within a monitoring zone and is expandable in the tree view. The Device Groups window allows operators to view, test and change the status of devices (readers, inputs and outputs).

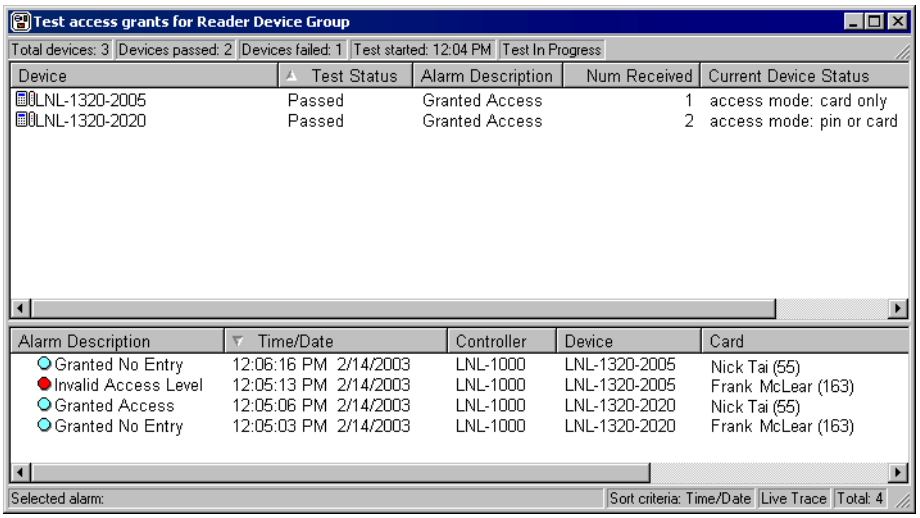
Toolbar Shortcut

To display the Device Groups Window, click the View Device Groups toolbar button or select **Device Groups** from the **View** menu



Device Group Test Mode Window

Similar windows display for the test access grants, test forced open and test inputs for device groups. The example below is a Test access grants for Reader Device Group window.



Field	Description
Upper status bar	Displays information about the upper display window and includes the total number of devices tested, the number of devices that pass and fail, what time the test started and the current status of the device test.
Upper display window	Displays the device name, test status, alarm description, number of inputs or requests received and the current device status. The information displayed in this window can be sorted by any column.
Lower display window	Displays a variety of user-defined columns that can be sorted. Users can select whether the following columns display: Alarm Description, Time/Date, Controller, Device, Input/Output, Card, Priority, Asset Scan ID, Asset Name, Intercom Station Called, Controller Time, Transmitter, Transmitter Input, Biometric Score, Account Group, Badge Type, Text, Line Number and Intrusion Area. For more information, refer to Select Column Configuration on page 58.
Lower status bar	Displays information about the lower display window and includes the name of the currently selected alarm, sort criteria, trace type and the total number of alarms listed.

Device Group Icons

The table below identifies the different icon groups available.

Icon	Description
	Access Control System

Icon	Description
	Alarm Mask Group
	Reader Group
	Alarm Input Group
	Alarm Output Group

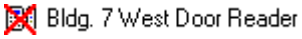
Hardware Device Icons

The table below identifies the different icon available.To view a list of icons and icon groups available in your database, as well as add or modify icons, open MapDesigner and select **Edit** > **Icon Library**.

Icon	Description
	Access Panel
	Alarm Input
	Alarm Output
	Alarm Panel
	CCTV Camera **Note:** The CCTV Camera icon flashes when there is motion detected with the associated camera. The CCTV Camera icon turns green when there is sound with the associated camera.
	CCTV Monitor
	CCTV Panel
	Fire Panel
	Function List
	Intercom Exchange
	Intercom Station
	Intrusion Area

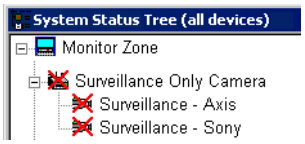
Icon	Description
	Intrusion Door
	Intrusion Offboard Relays
	Intrusion Onboard Relays
	Intrusion Panels
	Intrusion Zones
	Matrix Switcher
	Offline Lock Panel
	PC Panel
	Personal Safety Device Panel
	Reader
	Receiver
	Segment (only if your system is segmented)

Notes: An "X" through an icon indicates a broken connection, meaning that the software cannot communicate to the device. For example:



Although surveillance-only cameras are not associated with a physical video recorder, they are assigned to a virtual "surveillance-only recorder" to maintain consistency in the user interface. For example, the Alarm Monitoring hardware tree below shows two surveillance-only cameras

assigned to a virtually surveillance-only recorder which serves only as a placeholder to group cameras.



Device Status

Alarm Monitoring is the only application that displays the status of hardware devices. Alarm Monitoring obtains the status of a device from the Communication Server which in turn obtains the device status from hardware controllers.

Status icons are located to the left of hardware device icon. There may be one icon or a combination of icons, depending on the hardware status. The status is also displayed after the entry in parentheses.

Note: To view a list of current hardware status icons in your database, as well as add additional icons, open MapDesigner and select **Edit** > **Icon Library**

Device	Status	Icon
Best controllers and readers	Firmware download in progress	
Best readers and alarm panels	Serial number out of range	
	Device type mismatch	

Device	Status	Icon
Readers (Best and Apollo)	Online/offline	
	Door tamper	
	Reader tamper	
	Cabinet tamper	
	Power Failure	
	Forced open	
	Held open	
	Door contact fault	
	Reader mode	
	Reader verify mode	
	Cipher mode (Best only)	
	First card unlock mode	
	Extended held mode	
	Masked	
Readers (Best only)	REX fault	
Readers Aux Inputs	Active	
	Fault	
	Masked	
Reader Aux Outputs	Activated	
Alarm Inputs	Active	
	Fault	
	Masked	
Alarm Outputs	Activated	
Alarm Panels	Offline/online	
	Cabinet tamper	
	Power failure	
Intercom Stations	Busy	

Device	Status	Icon
Panel/Controller	Offline/online	
	Panel Memory Mismatch	
	Panel Memory Low	
	Panel database download in progress	
	Cabinet tamper	
	Power Failure	
	Panel type/Panel type mismatch	
	Panel options mismatch	
	Total memory, memory free	
	Max cardholders, current cardholders	
	Max assets, current assets	
	Max RSI templates, Current RSI templates	
	Last dialup time	
	Online with a plain connection	
	Online with encrypted connection	
	Online, but does not match the configured connection	
	Offline due to a standard connection problem	
	Offline due to an encryption problem	
	Dialup access controller is online with a plain connection	
	Dialup access controller is online with an encrypted connection	
	Dialup access controller, but does not match the configured connection	
	Dialup access controller is offline due to a standard connection problem	
	Dialup access controller s offline due to an encryption problem.	
Panel/Controller (Best hardware only)	Max Identix templates, current Identix templates	

Device	Status	Icon
Alarm Mask Group (Best and Apollo only)	Mask count	
Anti-Passback Area (Best and Apollo only)	Closed	
	Person count	

Procedures for Monitoring Devices

Update the Hardware Status

Hardware status information displays in several Alarm Monitoring windows. When alarms and actions occur in the system, B.A.S.I.S. software updates the status information "live" for the affected hardware. Operators can also choose to have the status updated on demand.

1. Select **Update All Hardware Status** from the **Control** menu or by right-click an alarm, access panel, alarm panel, alarm input, relay output or reader.
2. The update all hardware status feature polls the currently selected access panel and updates the hardware status of the associated devices. A message displays when the update is complete.

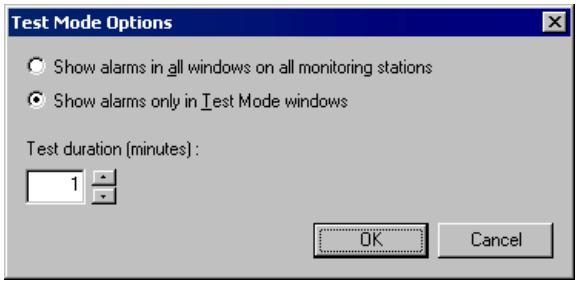
Note: If you are running Apollo hardware, there is a Hardware Status Update Frequency window to set automatic updates. You can set the frequency to No Updates, 10, 15, 20, 30 or 60 minutes (by selecting **Hardware Status Frequency** from the **Configure** menu).

Perform a Device Test

Operators can perform a test on various devices in the system. A special test mode operation is available for Input Groups, Reader Groups (Door Forced) and

Reader Groups (Access Grants). Performing this test allows you to see which devices generated alarms and which ones did not.

1. Display the Device Groups window by selecting **View** > **Device Groups**.
2. Right-click the device group and select the **Test Inputs**, **Test Door Forced** or **Test Access Grants**. If you select **Test Access Grants**, skip to step 7.
3. A dialog box appears:



4. You have two choices. Choose **Show alarms only in Test Mode windows** if you do not want the results to show up on any Monitoring Station. Otherwise choose **Show alarms in all windows on all Monitoring Stations**.
5. Type in the duration (in minutes) of the test. This option is available only if you selected **Show alarms only in Test mode windows**.
6. Click [OK] to initiate the test.
7. A Test Mode window launches. The top portion of the window lists all the devices being tested and their current status (whether the test was successful/ unsuccessful). Devices that failed the test flash in red. The bottom portion of the window displays a trace of the related alarms.
8. When the test is finished, all the windows and monitoring stations resume their normal display of alarms.

Note: Device status is not available for Matrix Switchers or Account Panels.

Locate or Search for a Device

Operators can locate or search for a device in any window in Alarm Monitoring.

1. Display any Alarm Monitoring window.
2. Verify your cursor is in the window.
3. Begin typing the name of the device. The system automatically scrolls to the first occurrence of those letters in column one.

View the Last Connection Time for Dialup Panels

The Last connect time status is displays in parenthesis after each dialup panel. It reflects the time of the panel's last "Communications Restored" event and is updated every time you disconnect from the panel.

To view a dialup panel's Last connect time within Alarm Monitoring:

- Locate the dialup panel in the System Status window. In parenthesis after the name of the dialup panel, the Last connect time is listed.

Last Connection Time Guidelines

The following are guidelines for the Last connect time status:

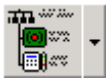
- If a dialup panel has never connected, the Last connect time for it is "Never".
- If a dialup panel connects while Alarm Monitoring is not running, the Last connect time for it is retrieved from the database when Alarm Monitoring starts up again.
- When a dialup panel is disconnected, the System Status window immediately reflects the new Last connect time regardless of whether the "Communications Lost" alarm is acknowledged or not.
- When a dialup panel and Alarm Monitoring station are in different time zones, the Last connect time displays both the local time and the panel time.

Download the B.A.S.I.S. Database or Firmware

Operators can download the B.A.S.I.S. database and/or firmware to devices via Alarm Monitoring. Devices include the controller, dual interface Rdr1 readers, BAS-1100 or BAS-1200 alarm panels, RS-485 command keypads, cameras and access panels.

Note: It is not possible to download firmware to single reader interfaces.

Toolbar Shortcut



1. Open Alarm Monitoring and display the System Status window by selecting **View** > **System Status** and then the desired window.
2. Right-click the access panel in the hardware view and select the **Download Database** or **Download Firmware**.

View the Firmware Type, Flash Chip Size, and DIP Switch Settings of a Controller.

The type of firmware a controller has is indicated in the firmware revision reported in the Alarm Monitoring hardware view. It can also be found in the diagnostic tab of the access panels folder in System Administration and in the main window of the Controller Encryption Configuration Utility, which can be found in the B.A.S.I.S. directory.

The flash chip size is indicated in the Alarm Monitoring controller properties dialog box, which you get to by right-clicking on the controller and selecting properties. It can also be found in the diagnostic tab of the access panels folder in System Administration and in the main window of the Controller Encryption Configuration Utility, which can be found in the B.A.S.I.S. directory.

Note: If the current firmware revision in the controller is older then 3.041 the controller will not report its flash size and it will not be indicated in any utility.

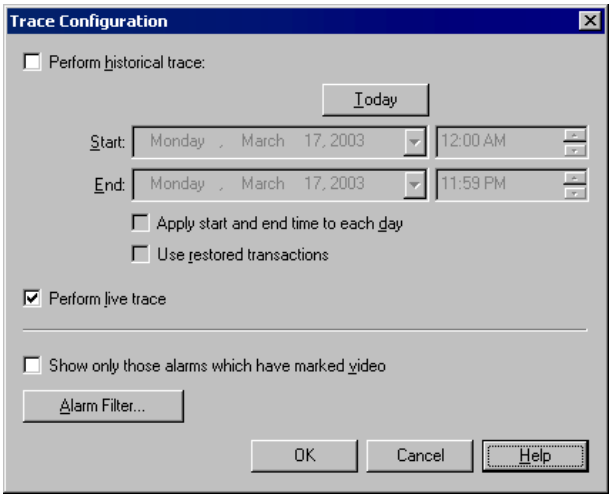
The current DIP switch settings for a given controller are indicated in the Alarm Monitoring controller properties dialog box, which you get to by right-clicking on the controller and selecting properties. It can also be found in the Diagnostic tab of the access panels folder in System Administration and in the main window of the Controller Encryption Configuration Utility, which can be found in the B.A.S.I.S. directory.

Chapter 6: Trace Alarms and Events

Trace Configuration Window

The Trace Configuration window performs live and historical traces of events and is displayed by:

- Selecting the **Trace** menu and then the type of device you wish to trace. Click [OK] when B.A.S.I.S. prompts you to verify the name of the device to be traced.
- Right-click an alarm and select **Trace** and then the device you wish to trace.



Trace Configuration Window

Field	Description
Perform historical trace	If the checkbox is selected, the trace will include events that occurred between the **Start** and **End** date/times you specify.
Today	When clicked, the **Start** and **End** fields populate with the following: • Start and End date: the current day's date • Start time: 00:00 on the current date • End time: 23:59 on the current date
Start	The first date/time combination that the trace displays events for
End	The last date/time combination that the trace displays events for

Trace Configuration Window (Continued)

Field	Description
Apply start and end time to each day	If the checkbox is selected, the time range is applied to each day within the date range. For example: A trace has a **Start** date/time of 12/1/1999 9:00 and an **End** date/time of 12/9/1999 17:00. • If the **Apply start and end time to each day** checkbox is checked, then the trace will include only those events that occurred during the hours of 9:00 a.m. through 5:00 p.m. on the days December 1st through December 9th, 1999. • If the **Apply start and end time to each day** checkbox is not checked, then the trace will include all events that occurred from 9:00 a.m. on December 1st until 5:00 p.m. on December 9th.
Use restored transactions	This option is applicable only when a historical trace is performed. • If the checkbox is selected, restored transactions will be included in the historical trace. • If the checkbox is not selected, normal transactions from the EVENTS table will be used for the historical trace.
Perform live trace	Controls whether new events are displayed or not • If the checkbox is selected, the trace displays new events. • If the checkbox is not selected, live tracing is disabled and new events are excluded from the trace.
Show only those alarms which have marked video	Controls whether alarms (events) that have marked video are displayed or not. • If the checkbox is selected, live tracing shows events that are new AND are configured (in the System Administration application) to have video marked for them. The marking is not instant, so the trace may not show the icon in front of the event right away. • When the **Show Only Those Alarms Which Have Marked Video** checkbox is checked and the **Perform Historical Trace** checkbox is checked, the trace will show events which have video marked for them, regardless of the current alarm-video configuration in the System Administration application. This means that a video-only trace may exclude some alarms seen in the main alarm view with a icon in front of them.
Alarm Filter	Enables you to configure the type of events that will be displayed for a trace. When clicked, the Alarm Filter window opens.
OK	Performs the trace using the settings selected and closes the Trace Configuration window. A Trace Monitor window will open, which looks identical to the Main Alarm Monitoring window, but displays only those alarms that are associated with the trace criteria specified.
Cancel	Cancels the pending requested action.
Help	Displays help for this topic.

Procedure for Tracing

Trace Alarms and Events

B.A.S.I.S. allows you to trace the alarms and events associated with a monitor zone, controller, device, badge, asset or area. This includes events from third party OpenIT sources.

1. Select (highlight) an alarm, event or device you want to trace.
2. Do one of the following:
   - Right-click and select **Trace**. Then select **Controller**, **Device**, **Badge**, **Asset** or **Area**.
   - From the **Trace** menu select **Controller**, **Device**, **Badge**, **Asset** or **Area**.
   - Click the toolbar button that corresponds to what you want to trace. Choices include:

     Traces a Controller

     Traces a Device (including alarm outputs, reader aux inputs and reader aux outputs)

     Traces a Badge

Note: If you are tracing a badge the Trace Badge window displays asking you to verify the Badge ID. Click [OK].

3. The Trace Configuration window displays.
4. To perform a historical trace, select the **Perform historical trace** checkbox and select the **Start** and **End** dates.
    a. **Optional** - You can also select the **Apply start and end time to each day** or the **Use restored transactions**.
5. To perform a live trace, select the **Perform live trace** checkbox.
    - **Show Only Those Alarms Which Have Marked Video** checkbox unchecked
6. To view only alarms with video select the **Show only those alarms which have marked video** checkbox.
7. Click [Alarm Filter] to select the types of events that will be displayed for this trace.
8. In the Alarm Filter window, select (place a checkmark beside) the alarm types you want displayed.
9. Click [OK].
10. In the Trace Configuration dialog, click [OK].
11. B.A.S.I.S. will open a new Trace Monitor window that looks identical to the Main Alarm Monitoring window, but only displays alarms that are associated with the trace.

Chapter 7: Video Monitoring

The Video Monitoring window displays live video only. To view recorded video you must use the Video Player.

The Video Monitoring window performs the following function:

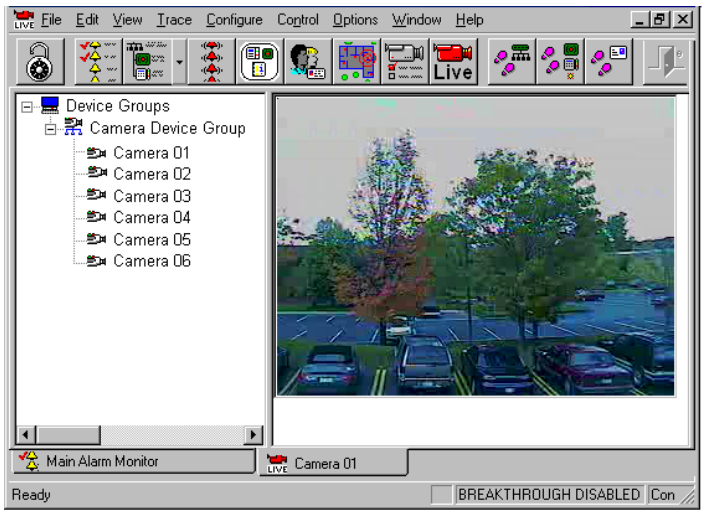
- Displays live video from one camera at any given time.

Toolbar Shortcut

The Video Monitoring window is displayed by:

- Selecting the Video Monitoring toolbar button.
- Selecting **View** > **Video Monitoring** from the menu.

Video Monitoring Window



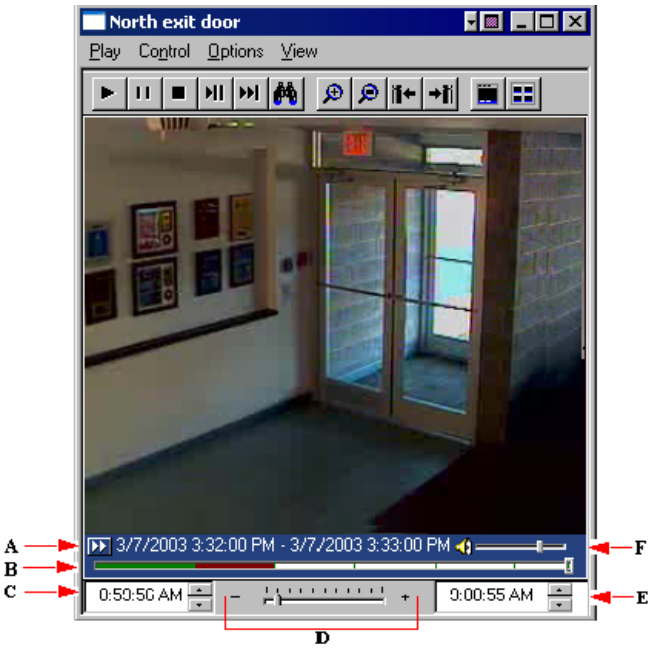
Field	Description
Device Groups listing	Lists the available video device groups. A device group can contain devices from more than one access panel. Device groups can also be segmented and belong either to one segment or all segments. If a device group belongs to only one segment, the group will contain only devices associated with the access panel defined for that segment.
Display area	Displays a specific camera view - live.

Video Player

The Video Player performs the following functions:

- Displays live or recorded video from one camera
- Displays live or recorded video from a group of cameras successively
- Displays video from a group of cameras or a recorder simultaneously.
- Displays recorded video associated with a video search
- Enables you to pan, tilt and zoom recorded and live video

The Video Player is displayed by right-clicking an alarm, device, camera or camera device group and selecting **Launch Video**.



Note: Refer to the Video Player Status Bar Table on on page 82 for the descriptions of the status bar components, A-F.

Video Player Menu and Toolbar Buttons Table

Field	Toolbar button	Description
Play menu		Contains the following menu options: **Live:** Plays live video from one or several cameras depending on the view settings. **Recorded:** Plays recorded video for the selected camera(s). **File:** Plays video clips from a file. **Note:** A checkmark displays beside the option that is active.
Control menu		Displays several options to play, pause and stop video as well as advance video, zoom in/out, adjust playback speed, search video and remove cameras from the Video Player window.
Options menu		Displays options to load video files, set start/end times to view recorded video, export video to a file, capture images from video and create video events.
View menu		Displays options to change how cameras views are displayed.
Play button		Plays recorded video.
Pause button		Pauses or temporarily stops playing recorded video.The video will continue from where it temporarily stopped when the play button is clicked.
Stop button		Stops playing recorded video and resets the player to the beginning of the video.
Frame Advance button		Advances video one frame at a time.
Fast Forward End button		Advances (fast forwards) video to the last frame.
Search Video button		Displays the Video Search window. This option is only available when the Video Player is playing recorded video. For more information, refer to Video Player on page 80.
Digital Zoom In button		Enlarges the view of a specific area in the Video Player and changes the focal point of the video to the location of the cursor. **Note:** To deselect this feature select **Digital Zoom In** from the **Control** menu.
Digital Zoom Out		Broadens the video view and changes the focal point of the video to the location of the cursor. **Note:** To deselect this feature select **Digital Zoom Out** from the **Control** menu.
Previous Camera		Displays the previous camera view. This feature only applies when you have opened multiple images and the Video Player is in single view mode.
Next Camera		Displays the next camera view. This feature only applies when you have opened the Video Player so that you can view multiple images and you are currently in single view.

Video Player Menu and Toolbar Buttons (Continued)Table

Field	Toolbar button	Description
Single View		Adjusts the Video Player to display a single camera view. The single view feature displays the first camera view regardless of which camera view is selected.
Matrix View		Enlarges the Video Player to display up to four camera views (two images across and two images down). Additional cameras can be seen using the scroll bar.
Display window		Displays live or previously recorded video.
Status bar		For information on the status bar please refer to Video Player Status Bar Table on on page 82.

Video Player Status Bar Table

Symbol	Field	Description
A	Date and time display	When live video is playing the status bar displays the camera name. When recorded video is playing the status bar contains two arrow heads . You can click the arrow heads to change the information displayed to any of the following: • Camera name • Video start date and time • Video start date/time and end date/time
B	Video display scroll bar	Move the scroll bar back and forth to view video at different dates/times. You do NOT need to pause or stop video to use the video display scroll bar. **Note:** Cameras configured with an LNVR recorder display different colors in the scroll bar for different types of recorded video. • **Red** - video is not available (e.g. a download was performed, LNVR was disconnected or restarted) • **White** - video is not being recorded (e.g. time lapse recording) • **Green** - video is being recorded (e.g. continuous recording or time lapse recording)
C	Start time	Video start time. Use this feature to adjust your video search.
D	Speed bar	Determines how fast the video is played as well as searched. Using the cursor click near the minus symbol to slow the video down or click the plus symbol to speed the video up. You can also adjust the speed by clicking and dragging the speed bar arm.
E	End time	Video end time. Use this feature to adjust your video search.

Video Player Status Bar Table (Continued)

Symbol	Field	Description
F	Volume	Sets the volume level for the camera with audio recording enabled. Only one camera video recorder can be enabled to record audio at one time. This applies to LDVR-SP, LDVR-SP4, LDVR-SP30, and LDVR-SP430 video recorders. For more information please refer to the Digital Video Folder chapter in the System Administration User Guide.

Video Search Window

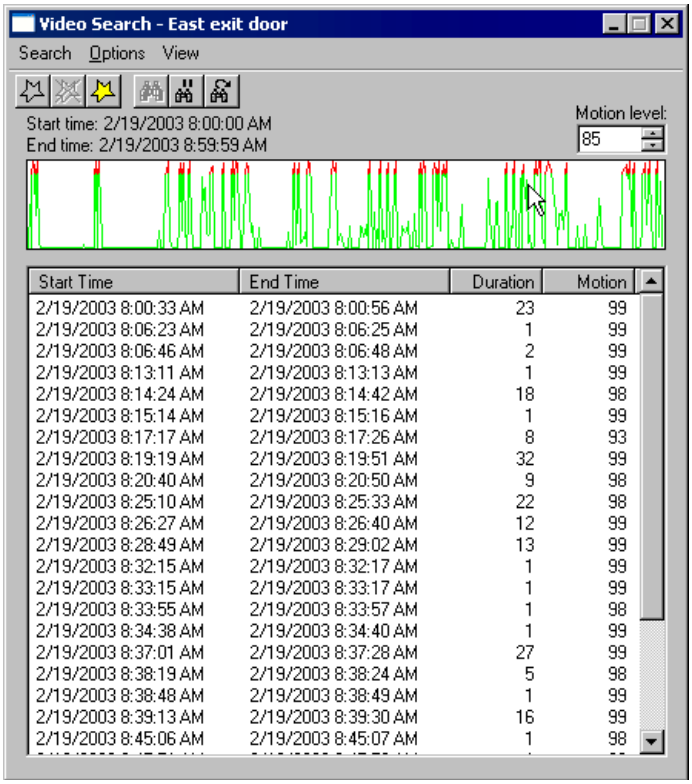
The video search feature looks for video on a recorder and the archive server that meets two criteria; a level of motion greater than or equal to a specified level and video that occurred within the time and date range specified. The video search process occurs on the client side, where the PC is running the Video Player. Search results are displayed as a detailed list or thumbnail images. Video from the search results are played using the Video Player.

The Video Search window performs the following functions:

- Analyzes recorded video for user-defined motion detection levels and reports the results in thumbnail images or a detailed list
- Searches recorded video for any event that meets user-specified criteria
- Enables recorded video that meets the search criteria to be played on the Video Player

Note: The video search feature is only available for LDVR recorders.

To display the Video search window please refer to Display the Video Search Window on on page 95.



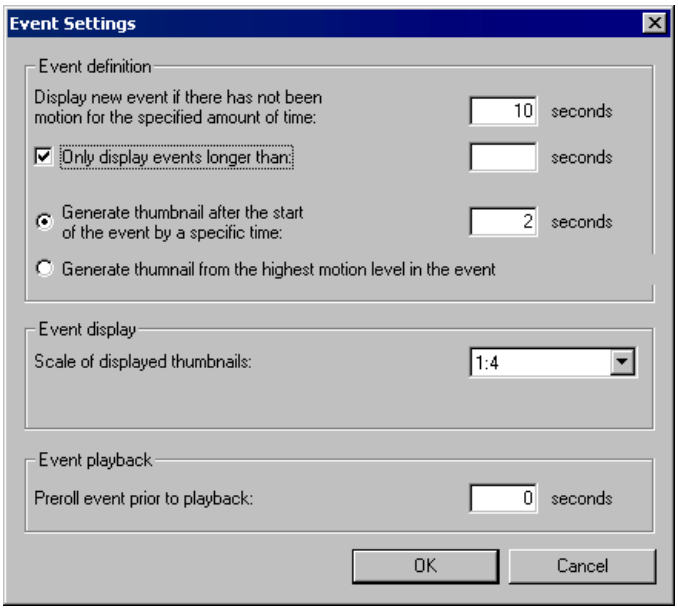
Field		Description
Search menu	 	Contains the following menu options: **Start:** Begins the video search and resumes the video search if it is paused. **Pause:** Pauses or temporarily stops searching video. The video search continues from where it temporarily stopped when the Start button is clicked. **Restart:** Restarts the video search at the beginning.
Options menu		Displays the **Event Settings** menu option which displays the Event Settings window. In The Event Setting window you can configure how the search results display. For more information, refer to Event Settings Window on page 87. **Note:** You may be prompted to restart the search when you change event settings.
View menu		Contains two menu options for displaying search results; **Images** or **Details**. In the screen shot above, the list view displays detailed information (Start Time, End Time, Duration and Motion level).

Field		Description
Create Motion Detection Region		Enables you to select a region in the Video Player to search. For more information please refer to Search Specific Portions of a Camera View on page 96. **Note:** This button is only available for Windows XP systems. **Note:** When you search video using the Motion Detection Region toolbar buttons, the yellow region the portion of the video that will be searched for motion detection.
Remove Motion Detection Region		Unselects any region in the Video Player you highlighted using the Create Motion Detection Region toolbar button. For more information please refer to Search Specific Portions of a Camera View on page 96. **Note:** This button is only available for Windows XP systems.
Include Motion Detection Region		Inverts the region you selected in the Video Player using the Create Motion Detection Region toolbar button. **Note:** This button is only available for Windows XP systems. **Note:** When you search video using the Motion Detection Region toolbar buttons, the yellow region the portion of the video that will be searched for motion detection.
Start time End time		The starting/ending point for the video search. This display only field is set in the Video Player under the **Options** menu. **Note:** If you change the start/end time in the Video Player, you must restart the video search for the new settings to apply.
Motion level		The minimum motion level required to be included in the search results. The motion level range is 0 to 100, where 0 represents no motion. The first and last frames of an event must have a motion level equal to or greater than the motion level value to be included in the search results.
Histogram		A color-coded graphical representation of motion levels. Red indicates a frame meets or exceeds the minimum motion level. Green indicates a frame is less than the threshold value. You can click any part of the histogram to view the corresponding recorded video. You do not need to wait for the search to complete to do so.
View area		The main part of the Video Search window that displays thumbnails or detailed information about search results. In this screen shot, the view area displays detailed information (Start Time, End Time, Duration and Motion level). You can double-click a thumbnail or an event in the view area to view the recorded video for that event (in the Video Player). You do not need to wait for the search to be complete to do so.

Event Settings Window

When searching for events, it is possible that an event occurs through out several frames. Therefore the user can make adjustments to the event settings to obtain the best results.

The Event Settings window is displayed by selecting **Event Settings** from the **Options** menu in the Video Search window.



Field	Description
Display new event if there has not been motion for the specified amount of time	Enter a time limit in seconds. If an event has an interval without motion longer than the value entered, it displays as multiple events. Increasing the amount of time decreases the number of frames that meet or exceed the minimum motion level and therefore the number of red lines displayed in the histogram.
Only display events longer than	Filters the event list. This is useful in situations where there is extraneous noise. For example, when artificial lighting is unstable and flickers causing the video camera to capture the event. Displaying events that are longer than one or two seconds is an effective way to remove such noise.
Generate thumbnail after the start of the event by a specific time	Generates a thumbnail image after the specified amount of time.
Generate thumbnail from the highest motion level in the event	Generates a thumbnail image from the highest motion level in the event.
Scale of displayed thumbnails	Specifies the scale of thumbnails displayed in the Video Search window. Options include a 1:1 ratio, where the thumbnail is the same size as the image in the Video Search window, down to a 1:8 ratio, where thumbnail is 1/8th of its original size.
Preroll event prior to playback	Specifies the preroll time when the user plays back events.

Field	Description
OK	Applies the event settings and closes the Event Settings window.
Cancel	Closes the Event Settings window without applying any changes.

Video Search Performance Requirements

A fast network, 100 Mbps or greater, is recommended between the site where video is located and the site where the computer running the Video Player is located. A fast network is recommended because all video is analyzed on the client side, therefore the faster video can be transmitted from the server side, the faster the search will be.

The hard drive speed on the server side must be able to support the number of clients using the server. Clients include Video Players and archive servers.

A fast CPU on the client computer is also recommended. This is primarily due to the motion detection feature. In some cases, when the network and server side hard drive are fast enough, the CPU on the client side can be the bottleneck. A Pentium III based computer is required although a Pentium IV computer is recommended.

Video Monitoring Procedures

aLaunch Video (Live/Recorded) From a Camera

1. To launch video in Alarm Monitoring complete one of the following:
   - In an alarm window right-click an alarm and select **Launch Video**.
   - In a map or System Status window right-click a device icon and select **Launch Video**.
   - In the Device Group window right-click a camera icon and select **Launch Video**.
   - In the Video Monitoring window double-click an online camera or right-click a camera icon and select **Launch Video**.
   - Drag and drop a camera, camera device group or recorder into the Video Player. This launches ALL of the video cameras in that particular group or recorder (up to 32 cameras at once).
2. To view live video select **Live** from the **Play** menu.
3. To view recorded video select **Recorded** from the **Play** menu.

Load and View a Video File

1. Display the Video Player. For more information please refer to Video Player on page 80.
2. Select **Load File** from the **Options** menu.
3. The Open window displays. Select the correct ".info" file, and click [Open]. The recorded video automatically plays.
4. To replay the video file click the Stop toolbar button and then click the Play toolbar button.

Monitor Video in Matrix View

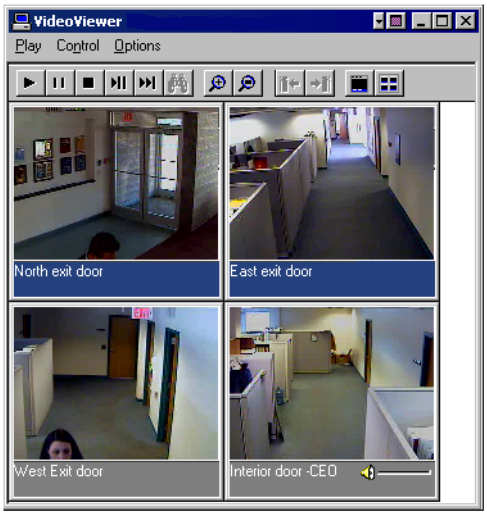
The Video Player in matrix view can be used to view live or recorded video from multiple cameras simultaneously.

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera in the Video Player on on page 88.
2. The Video Player displays. From the **View** menu, select **As Matrix**. You can also select the **Matrix View** toolbar button.

Note: Matrix view displays up to 32 cameras. There may be more cameras available than what fits in the viewable area. You may scroll or resize the window to view additional cameras. To resize the window hover the pointer over the corner or edge of the window until a double-headed arrow displays. Then drag the window to its desired size.

---

3. The screen below displays Matrix view.



Note: When viewing multiple cameras simultaneously, please note that the system automatically displays each window in such a way that it is active (the status bar for each window is blue.) Therefore any command will be applied to

every window. To deselect a window, place the cursor in the window and click. The status bar is gray when the window is deselected.

Monitor Video of Multiple Cameras (Successively)

You can use the Video Player or the Video Monitoring window to monitor video of multiple cameras successively. To monitor video using the Video Monitoring window, please refer to View the Video Tour on on page 91. To monitor video of multiple cameras successively using the Video Player:

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera in the Video Player on on page 88.
2. Click and drag every camera or camera group, you will want to view, into the Video Player the video.
3. From the **View** menu select **Camera**. A sub-menu displays. Select the desired camera view.

Toolbar Shortcuts

4. Repeat step 3 to view different cameras successively or click the Previous Camera and the Next Camera toolbar buttons.

Monitor Video of a Specific Camera

To monitor video of a specific camera in Alarm Monitoring complete one of the following:

- In the Video Monitoring window double-click an online camera to view live video.
- In an alarm window, map or System Status window right-click a device icon and select **Launch Video** to view live or recorded video.
- In the Device Group window right-click a camera icon and select **Launch Video** to view live or recorded video.
- In the Video Monitoring window double-click an online camera or right-click a camera icon and select **Launch Video**.
- Drag and drop a camera into the Video Player.

Toolbar Shortcut

- If the Video Player is matrix view, click the Single View toolbar button. Click the Previous Camera or Next Camera toolbar buttons to view a specific camera.
- In the Video Player select **Camera** from the **View** menu. A sub-menu lists the currently displayed cameras. Select the camera of your choice.

About Surveillance-only Cameras

Surveillance-only cameras (stand-alone IP cameras) support live video only, they cannot record or playback video or support PTZ, whereas IP cameras (Internet Protocol cameras) support all of these features. IP cameras are directly connected to the network with their own IP address. They do not need to be connected to a

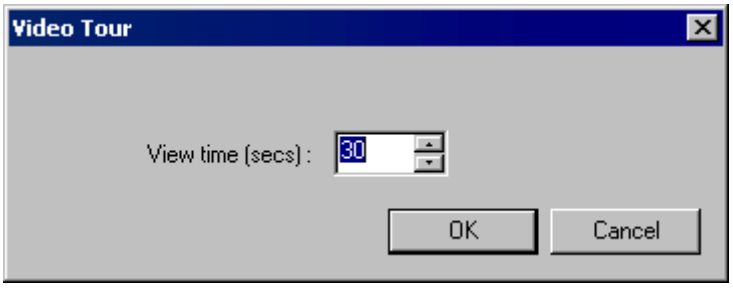
computer or a video capture card. More advanced IP cameras may provide additional functionality such as a built-in web server, motion detection, alarm inputs/outputs and e-mail and FTP support.

View the Video Tour

The Video Tour is used to view a group of cameras successively. These cameras are defined as a device group in the Groups folder of System Administration. The Video Tour feature is only available for online cameras/recorders.

Toolbar Shortcut

1. Launch the Video Monitoring window by either selecting the Video Monitoring toolbar button or choosing **Video Monitoring** from the **View** menu.
2. Verify the cameras/recorders are online. If the device icon does not have a red "X" through it the device is online.
3. Right-click a camera device group and select **Configure Video**. The Video Tour window displays.

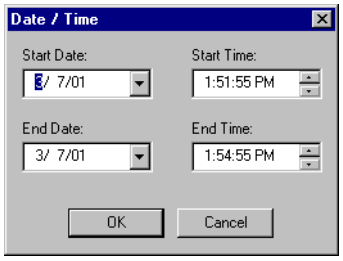


4. Select the desired View time and click [OK]. This is the amount of time each camera is displayed in the tour.
5. Right-click the camera device group again and select **Start Tour**. The right side of the window displays the camera views.

Set Start and End Dates

The following procedure applies to recorded video.

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera on on page 88. Verify recorded video is playing in the Video Player.
2. Select **Set Start/End Date** from the **Options** menu.
3. The Date / Time window appears. Fill in the appropriate dates and times and click [OK].



Note: Use your keyboard to quickly navigate between fields in the Date / Time window. The right and left arrow keys allow you to navigate from minutes to seconds. The up and down arrow keys allow you to switch between AM and PM. The tab key allows you to navigate between fields (Start Date, Start Time, End Date and End Time).

Export Video To A File

To convert video to ".afs" files refer to disc 2 of your B.A.S.I.S. installation CDs.

Recorded video and audio can be saved/exported to a file. By default the video clip is saved as ".info" and ".spfs" files for LDVR hardware or ".lnr" files for LNVR hardware.

Note: Using the conversion utility, available on the B.A.S.I.S. Installation CDs disc 2, video is converted/exported as an ".afs" file which can be played on any Microsoft Windows Media Player.

1. While viewing recorded, in the Video Player, select **Set Start/End Date** from the **Options** menu.
2. The Date / Time window appears. Fill in the appropriate dates and times and click [OK]. For more information please refer to Set Start and End Dates on page 91.
3. From the **Options** menu select **Export Video**. The Save As window displays.
4. Select the file location. Enter the filename and click [Save].

Capture an Image

You can capture images from live and recorded video. Images are saved as ".JPG" files.

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera in the Video Player on page 88.
2. Verify one camera view is selected; the status bar for a selected camera is blue - not gray.
3. From the **Options** menu select **Capture Image**.
4. The Multimedia Capture window displays.
5. Click [Export]. The Save As window displays.
6. Enter a file name and click [Save]. If the photo is bitmapped and the crop window is used, the portion of the image within the cropped area is saved. Otherwise, the whole photo is saved.
7. Click [OK].

Create a Video Event

Video events are automatically created in Alarm Monitoring if a camera is correctly added to a video recorder, hardware is linked to the camera and an alarm - video configuration is established.

You can also manually create a video event to lock/mark video at the exact start and stop times you desired. For example, if the B.A.S.I.S. system automatically creates an event for a door forced open, but you want the event to include 5 seconds after the event occurred, you can review the video and manually create an event at the desired times.

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera on on page 88. Verify the recorded video is playing in the Video Player.
2. If necessary use the toolbar settings and the start and stop time fields to identify the portion of video to be marked as an event.
3. From the **Options** menu select **Create Video Event**. The Alarm Monitoring window displays a User Generated Video Event alarm.

Switch Camera Views Displayed in Video Player

Cameras and device groups can be dragged and dropped from the camera list into the Video Player for viewing.

Switch Between Camera and Monitor Views

This feature applies to Nice Vision recorders with configured monitors.

1. Right-click a camera or monitor.
2. The popup menu appears. To view monitors, choose **Switch To** and select the monitor from the list that appears. To view cameras, choose **Display** and select the camera from the list that appears.

Pan, Tilt and Zoom

The screen below shows the addition of a Pan, Tilt and Zoom (PTZ) control into the Video Player. The Video Player can be used to control PTZ devices if the PTZ device is connected to a Digital Video Server and a Matrix Switcher.

Note: Cameras are configured to be connected to a Matrix Switcher in the System Administration software application. From the **Video** menu select **Digital Video** and then the **Camera** tab.

- **Using the PTZ Toolbar.** The PTZ Toolbar contains a Pan and Tilt control that can be used to pan or tilt a camera. Once PTZ is activated, the buttons can be used to zoom in or out, move and focus the camera. The user can also press and hold any of the zoom, focus or iris buttons to achieve the preferred view.

- **Using the Mouse.** You can manipulate the Pan, Tilt and Zoom controls by right or left clicking your mouse in the video window. A left mouse button click causes the camera to move toward the cursor. The camera keeps moving in that direction until the mouse button is released. If you right-click in the top half of the screen the camera will zoom in until the mouse is released. Clicking and holding the mouse in the bottom half of the screen causes the camera to zoom out. The farther away from center the mouse is the faster the device will pan, tilt or zoom. If you have a scroll mouse moving the scroll wheel up will zoom in and moving the scroll wheel back will zoom out.

- **Using the Keyboard.** You can use your keyboard arrow keys to pan, tilt and zoom. The left and right arrow keys pan the camera left and right. The up and down arrow keys tilt the camera up and down. Holding the <Shift> key

down while pressing either the up or down arrow causes the camera to zoom in or zoom out.

Display the Video Search Window

The Video Search window is a modeless dialog box that enables operators to search video and monitor alarms without closing the Video Player or Video Search window.

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera in the Video Player on on page 88. Verify the recorded video is playing in the Video Player.

Toolbar Shortcut

2. Click the Video Search toolbar button or from the **Control** menu select **Video Search**. The Video Search window displays.

Search Video

You can search video using the Video Player and Video Search window.

1. Follow the procedures to aLaunch Video (Live/Recorded) From a Camera on on page 88. Verify the recorded video is playing in the Video Player.
2. From the **Options** menu select **Set Start/End Date**.
3. The Date / Time window displays. Enter the desired date and time ranges you wish to search and click [OK]. For more information please refer to Set Start and End Dates on page 91.
4. Notice the Video Player immediately plays the recorded video starting with the start date and time specified. To search video, within the date range, that has a specified level of motion complete the remaining steps.
5. From the **Control** menu select **Video Search** or click the Video Search toolbar button. The Video Search window displays.
6. From the **View** menu select the desired view; images or details. The active view contains a checkmark beside it.
7. From the **Options** menu select **Event Settings**. Make the desired setting changes and click [OK]. For more information please refer to Event Settings Window on page 87.
8. If you receive a warning that you must restart the search for the new settings to take affect, click [OK].

Toolbar Shortcut

9. From the **Search** menu select **Start** or click the Start toolbar button.

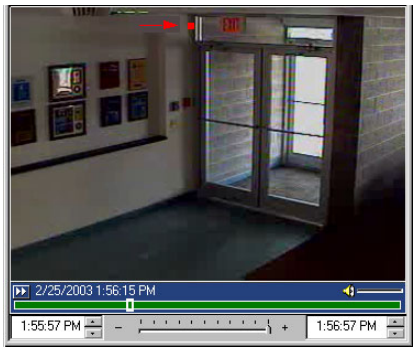
Search Specific Portions of a Camera View

The Video Search window has toolbar buttons that enable you to search for motion within a selected portion of a camera view.

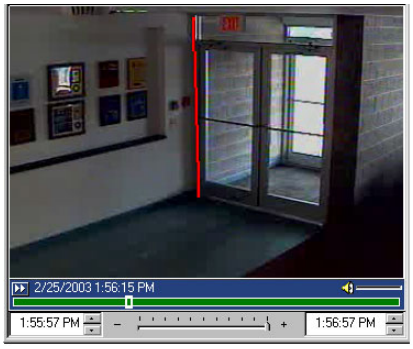
Toolbar Shortcut

1. Display the Video Search window. For more information please refer to Display the Video Search Window on page 95.
2. Click the Create Motion Detection Region toolbar button.
3. In the Video Player left-click to create a starting point for the area you want to highlight. A red dot displays.

Note: The examples below are enhanced for visibility. When you complete this procedure, the area highlighted may be hard to discern until a line is drawn.



4. Click another point in the area you want to highlight. A red line connecting the two points displays.



5. Continue clicking points to expand the highlighted area.

Note: If at any time you want to remove the highlighted area, go to the Video Search window and click the Remove Motion Detection Region toolbar button. All highlights are removed.

6. When you are satisfied with the highlighted area go to the Video Search window and click the Search toolbar button. Only the highlighted area is searched.
7. You can also invert the area you highlighted by clicking the Include the Motion Detection Region in the Search toolbar button. In the example above, everything but the entrance door would be highlighted.

View Search Results

There are several ways to view the recorded video associated with the video search results. All video is displayed in the Video Player.

From the Video Search window:

- Click any part of the histogram.
- Double-click a thumbnail or listed event.

Filter Search Results

After the initial search is performed you can continue to filter the results by changing the motion level in the Video Search window.

If you increase or decrease the motion level, the Video Search window will display the images/details from the initial search that are equal to or greater than the new minimum motion value. It will not display all the recorded images that are equal to or greater than the new minimum motion value. In order to do that you must restart the search.

Chapter 8: Video Verification

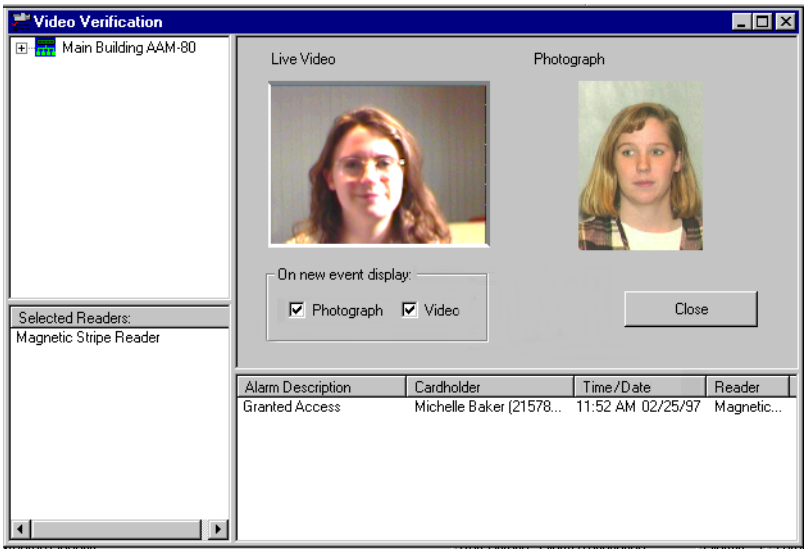
Video verification is the process of comparing "live" (as it is happening) video with a photograph stored in the database. When a person swipes a badge through a reader, you can use video verification to compare the person's appearance with the photograph that was taken to create the badge.

Displayed by:

The Video Verification window can be displayed several ways:

- Select the Video Verification toolbar button.
- From the **View** menu select **Video Verification**.

Video Verification Window



Form element	Comment
Panels/readers window	Lists all panels and readers in the system.
Selected readers	Contains those readers from which the Video Verification window will receive information. If this list is empty, no alarms will display in the Video Verification window.
Live video	Displays live video from a CCTV (camera) device at a specific location. • If you see a black box instead of live video, it means that either there is no camera available or the camera isn't working properly. • If you see a "Live video not available" message, it means that your System Administrator has made live video from that location unavailable to Alarm Monitoring stations.
Photograph	Displays a specific cardholder record photo.

Form element	Comment
On new event display	Includes the **Photograph** and **Video** checkbox fields. • **Video**: If checked, pan, tilt and zoom CCTV commands are automatically enabled. If unchecked, pan, tilt and zoom CCTV commands must be manually invoked. Live video remains visible regardless of the state of this checkbox. • **Photograph**: If checked, as each new alarm arrives, the corresponding cardholder photo displays.
Alarms window	Lists alarms as they arrive. Each row represents one alarm. Click the following column headings to arrange alarms by that heading: • **Alarm Description**: Name of the alarm • **Cardholder**: Cardholder's name and Badge ID • **Time/Date**: Time and date the alarm occurred. The way that the time and date are displayed varies according to the time/date settings chosen in the Windows Control Panel on your computer. • **Reader**: Reader at which the alarm occurred Resize the width of a column by positioning the mouse pointer over the boundary of two column headings. Then click and drag to resize the column.
Close	Closes the Video Verification window.

Video Verification Procedures

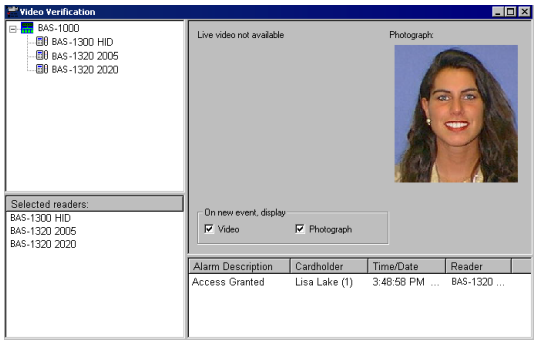
Add or Remove Readers

To add or remove readers using the video verification window, the reader must be added to the Selected Readers list.

Note: The Panels/Reader list is located in the upper left portion of the Video Verification window. The Selected Readers list is located in the lower left portion of the Video Verification window.

- To add an entry to the Selected Readers list, double-click the reader in the Panels/Readers list.
- To add a entry to the Selected Readers list, select one or more alarm(s) before you open the Video Verification window, the corresponding reader(s) will be added automatically.
- To add all the readers associated with a particular panel, double-click the panel entry in the Panels/Readers list.

- To remove a reader from the Selected Readers list, double-click the reader's entry in the Selected Readers list.



Display the Cardholder Photo and Live Video

Clicking an alarm in the video verification alarms window displays both the cardholder photo and live video from a camera at the reader. Live video continues to display until one of the following happens:

- You click another alarm.
- Another alarm arrives (this is true only if the **Video** checkbox is selected.)

Notes: The **Video** checkbox must be selected to display live video when a new alarm occurs.

The **Photograph** checkbox must be selected to display the cardholder's photograph when a new alarm occurs.

Delete an Alarm in the Video Verification Window

- To remove an alarm from the alarms window, click the alarm then select **Delete** from the **Edit** menu or right-click the alarm and select **Delete**.
- To clear all alarms from the alarms window, select **Delete All** from the **Edit** menu.

Chapter 9: Control Devices and Areas

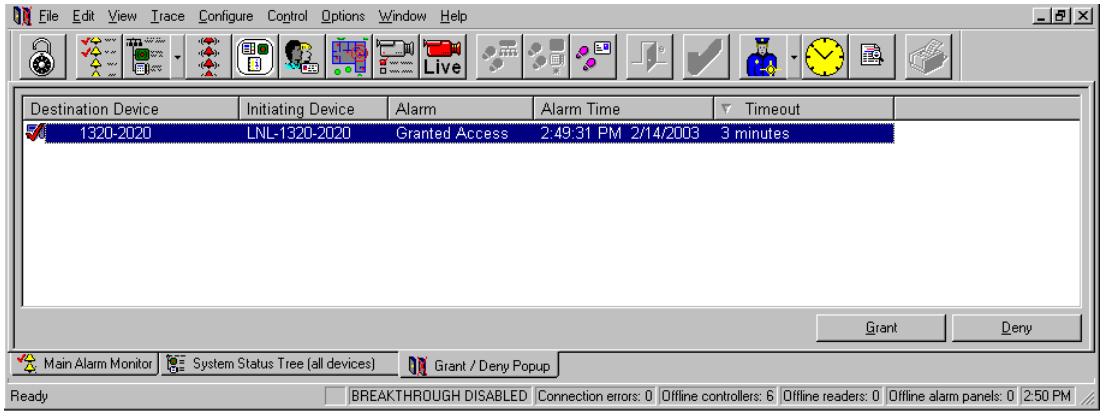
Permissions for control device groups can be given or restricted through System Administration. From the **Administration** menu select **Users**. On the Monitor Permission Groups sub-tab there is a Control Device Groups sub-tab with which you can control access to device groups.

Grant / Deny Pop-up Window

Your System Administrator can configure any input event for any device to execute an output action that launches a grant/deny pop-up window associated with a door/reader. Alarm Monitoring operators with the correct permissions can either grant or deny access through the door/reader. When a grant is issued the door is pulsed open. When a deny is issued, no command is sent.

Note: For configuration procedures refer to the Global I/O Folder chapter in the System Administration User Guide.

Alarm Monitoring stations and operators monitoring the same zone the input device/event and output device/event are configured for are notified when the input event occurs.



Field	Description
Display area	Displays any and all active requests. The display window contains the following columns: • **Destination Device** - The door/reader the output action will affect. • **Initiating Device** - The device the request is coming from. **Note:** Both the initiating device and destination device must be in the same monitor zone. • **Alarm** - The input event that is linked to an output action. • **Alarm Time** - The time the request was initiated. • **Timeout** - The total amount of time the operator has to either grant or deny the request. The timeout value is user-defined with a default value of 3 minutes. This field does not refresh. To determine the amount of time remaining the operator must also refer to the Alarm Time column and the current time located in the status bar to determine when the request was initiated.
Grant	Grants the request (pulses open the door) and removes the request from the Grant / Deny pop-up window.
Deny	Denies the request (no command is issued to the hardware) and removes the request from the Grant / Deny pop-up window.

Grant / Deny Pop-up Window Procedures

Grant or Deny Access

1. Verify the Communication and Linkage Server are running. To do this, click the Start button then select **Programs** > **B.A.S.I.S. ET** > **Communication Server** or **Linkage Server**.
2. To grant access, complete one of the following when the Grant / Deny pop-up window displays:
   - Double-click a request.
   - Right-click a request and select **Grant**.
   - Select (highlight) a request and click [Grant].

Note: You must have the open door user permission in order to issue a grant. Contact your System Administrator to set up this permission or refer to the

Users Folder chapter in the System Administration User Guide for procedures.

3. To deny access, complete one of the following when the Grant / Deny pop-up window displays:
   - Let the timeout value expire by doing nothing.
   - Right-click a request and select **Deny**.
   - Select (highlight) a request and click [Deny].

Note: A user transaction is logged when a grant or deny occurs.

Right-click Options to Control Devices and Areas

You can control devices and areas through a wide variety of right-click and left-click menu options available in Alarm Monitoring. You can right-click and left-click icons in map view, right-click alarms, right-click device groups as well as right-click and left-click hardware in the System Status window. The menu options available when you right-click or left-click depend on the window you are in and the device or area you are clicking on.

Some right-click and left-click menus contain sub-menus. To execute commands you must first select the device from the right-click or left-click menu. A sub-menu of options displays to control that device.

Note: Many of the right-click and left-click options are also available as options from the main menu.

General Right-click Options

These right-click options can be available for alarms as well as multiple devices/ hardware.

- **Acknowledge** - acknowledges the currently selected alarm.
- **Trace** - traces the selected device.
- **Update Hardware Status** - polls currently selected access panel/controller and updates the hardware status. If a downstream device (like a reader) is selected, the update hardware status is done for the controller associated with that device.
- **View Map** - displays a map associated with the selected device (if one exists). If more than one map exists, the user is prompted to select a map.
- **Launch Video** - displays video for the selected device if a camera is associated with the device.

Monitor Zone Right-click Options

- **Update All Hardware Status -** updates the display to show the currently status of all devices.
- **Set All Controller Clocks** - sets all clocks to the current system time.
- **Trace Monitor Zone** - traces a monitor zone.

Access Panel and Alarm Panel Right-click Options

- **Properties** - available for access and intrusion panels.
- **Open Door(s)** - opens the door(s) associated with the selected access panel. If using Recognition Source readers this option will not be available, because these specific readers are not in constant communication with the PIM devices.
- **Set Controller Clock** - sets selected access panel/controller clock to current time. If a device other than an access panel/controller is selected, this option sets the clock on the access panel/controller to which the device is attached.
- **Reader Access Modes** - updates the reader mode of every reader associated with selected access panel/controller or reader.
- **Reader Verify Mode** - used to enable or disable verify mode for access control readers with an associated secondary reader. When verify mode is enabled, access to both the primary and secondary reader is required. When verify mode is disabled, only access to the primary reader is required.
- **Activate** - activates the outputs associated with the selected access panel.
- **Deactivate** - deactivates the outputs associated with the selected access panel.
- **Pulse** - pulses all outputs associated with the selected access panel.
- **Mask** - masks inputs or alarms for the currently selected reader.
- **UnMask** - unmasks inputs or alarms for the currently selected reader.
- **Download Firmware** - downloads firmware to the selected controller, BAS-1100 or BAS-1200 alarm panel or RS-485 command keypads. Contollers and gateways display firmware revision numbers using three decimal places, while downstream devices display the firmware revision number using two.
- **Download Database -** downloads the database to the access panel/ controller.
- **Reset Use Limit -** resets the number of times a badge can be used on a particular access panel/controller.
- **Connect -** connects the access panel/controller via a dialup/modem connection.
- **Disconnect -** connects the access panel/controller via a dialup/modem connection.

Intrusion Panel and Relay Right-click Options

In addition to the acknowledge, trace, update hardware status, properties and set controller clock right-click options, intrusion panels and relays can also have the following right-click option.

- **Execute Custom Function** - executes a custom function associated with the Radionics Intrusion Controller. This menu option is only available with Radionics Intrusion Controllers.

Intercom Right-click Options

- **Place Call** - displays a dialog box where you enter the station number you are calling to.
- **Cancel Call** - cancels the intercom call.
- **Badge Information -** displays badge information associated with the intercom event; who placed the call and/or who received the call. If an intercom event has two intercom stations associated with it (the station that placed the call and the station that received the call) a dialog displays, allowing alarm monitoring operators to select the intercom station(s) they want to base the cardholder search on.

Note: The Badge Information right-click option is only available for intercom stations linked with the customized cardholder field, Cell number. For more information, refer to the Cardholder Options folder - Automatic Lookup form in System Administration.

Reader Right-click Options

In addition to several options listed in Access Panels and Alarm Panels, right-click options for readers also include:

It is not possible to download firmware to single reader interfaces.

- **Download Reader Firmware** - downloads firmware to the selected dual interface Rdr1 reader. Displays the major and minor firmware revision number. The minor firmware revision number displays as the last two digits
- **Reader Biometric Verify Mode** - enables/disables verify mode for access control readers with an associated biometric reader. When verify mode is enabled, the normal card and/or pin access is and a biometric match is required. When verify mode is disabled, only the card and/or pin access is required.
- **Reader First Card Unlock Mode** - enables/disables the Reader First Card Unlock Mode. The Reader First Card Unlock Mode is a qualifier for online Reader Mode. When enabled, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked.

Note: Reader First Card Unlock Mode is only supported on the BAS-2000 controller. However, first style unlock behavior can be configured for use with any access controller through Best's Global I/O Support.

Alarm Mask Group Right-click Options

- **Group Mask** - masks inputs or alarms for the currently selected reader.
- **Group Unmask** - unmasks inputs or alarms for the currently selected reader.

Function List Right-click Options

Function Lists are keypad - activated commands that are programmed into an access panel. Function lists can be accessed by assigning them to specific keypad sequences.

- **Clear All Terms** - only applicable to Apollo function lists. Used to clear all terms, and set all the resulting function list values to false.
- **Execute: True** - sets the logic term to true.
- **Execute: False**- sets the logic term to false.
- **Execute: Pulse** - temporarily sets the logic term to true.

Action Group Right-click Options

In addition to the view map option, action groups also include execute as a right-click option.

Note: Action groups will display if the logged in user has the segment access to the action group along with permissions to execute all of the actions in the action group.

Anti-Passback Area Right-click Options

These right-click options are unique to areas and area alarms. There are other right-click options available for areas and they are listed in General Options.

- **Update Area Status** - updates the status of both safe and hazardous areas so that operators can have a current view of cardholder locations.
- **Occupancy Report** - provides a current report of the cardholders currently in a safe area.
- **Move Badges** - enables an operator to manually move all the badges in one area to another.
- **Mustering Report** - provides a current report of the cardholders currently in a hazardous area.

- **Start Muster Mode** - initiates Muster mode. The Start Muster Mode window displays and provides an area to enter comments.
- **Reset Muster Mode** - ends Muster mode. The Reset Muster Mode window displays and provides an area to enter comments.

Guard Tour Right-click Options

These right-click options are available if Guard Tour is set up in your system.

- **Launch Tour** - starts a guard tour.
- **View Tour** - displays the guard tour live tracking window for a specific tour.

Cisco Hardware Right-click Options

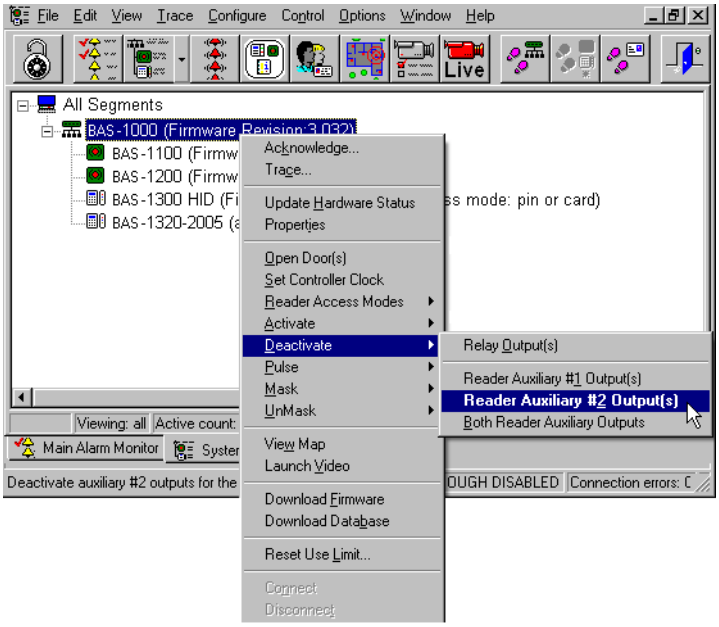
If you right click on an output in the hardware view (either list or tree), you see options for Cisco AIC outputs.

- **Momentary On -** sets the output in the On state momentarily for the duration specified, and then returns to its previous state.
- **Momentary Off** - sets the output in the Off state momentarily for the duration specified, and then returns to its previous state.
- **Latched On -** sets the output in the On position permanently.
- **Latched Off -** sets the output in the Off position permanently.

Single and Double Left-click Mode

Each Alarm Monitoring operator can set their options so that commands are executed with a single left-click or a double left-click of an icon in the system status view or map view. The default setting is to execute commands with a double left-click.

Furthermore, if that command was previously available as a right-click menu option, then the command will be listed in bold when the device is right-clicked. For some menus, the default command may be in a sub-menu of the context menu. The example below shows the **Reader Auxiliary Output # 2** in bold. This is the command that will be executed when the operator single or double left-clicks the controller icon, depending on how they have set their options.



Note: Using the System Administration application your System Administrator can associate commands with a device or area icon so that when the icon is single or double left-clicked in Alarm Monitoring, the command is executed. For information on how to associate a command with a device or area icon, refer to the Monitoring Options Folder Chapter in the System Administration User Guide.

Activate Single or Double Left-click Mode

Single or double left-click mode is configurable per user.

To activate single left-click mode select (place a checkmark beside) the **Execute Command on Single Click of Icon** in the **Options** menu of Alarm Monitoring. While in this mode you can single left-click an icon in the Alarm Monitoring system status and map view to execute the command configured for that device or area.

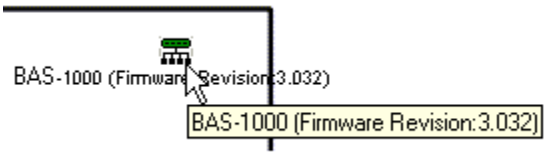
To activate double left-click mode deselect (there is no checkmark beside) the **Execute Command on Single Click of Icon** in the **Options** menu of Alarm Monitoring.

Select a Device in Single or Double Left-click Mode

Single Left-click Mode

In single left-click mode you can select a device, by placing or hovering the cursor near the device without left-clicking. The system status list and tree view identifies a selected device by underlining and/or highlighting the device.

The map view identifies a selected device by displaying the tool tip.



Double Left-click Mode

To select a device in double-click mode, left-click the device.

Execute a Command in Single or Double Left-click Mode

Single Left-click Mode

To execute a command in single left-click mode, left-click the device. Clicking the expand symbol in tree view does not execute the command.

Double Left-click Mode

To execute the command, double left-click the device.

Note: If you are in double left-click mode in the System Status view, not only do you execute the command when you double left-click a device, but you also expand or collapse the hardware list.

Chapter 10: Monitor Alarms

When an alarm occurs, it displays in the Main Alarm Monitoring window. Each alarm displays in its own row and is preceded by a colored dot. If alarms are configured in the System Administration software so that they do not automatically delete after they are acknowledged, an alarm icon will also display beside the colored dot after it is acknowledged.

Alarm Icons

The following table is a list of the different types of alarm icons.

Icon	Description
	Alarm acknowledged without notes.
	Alarm acknowledged with notes.
	An outstanding acknowledgment action is associated with the alarm. An *acknowledgment action* is an action that will automatically be carried out when the alarm is acknowledged.
	A camera is associated with the device that the alarm occurred on/for. Therefor you can pull up live video via the **Launch Video** right-click menu option.
	Alarm acknowledged without notes and a camera is associated with the device.
	Alarm acknowledged with notes and a camera is associated with the device.
	An outstanding acknowledgment action is associated with the alarm and a camera is associated with the device.
	The digital video associated with the alarm has been marked.
	Alarm acknowledged without notes and has archived video.
	Alarm acknowledged with notes and has archived video.
	The alarm has outstanding acknowledgment actions and archived video.

Pending Alarms Window

The Pending Alarms window is similar to the Main Alarm Monitoring window in that it has the same menu options and toolbars. However, the Pending Alarms window only displays *pending alarms*, alarms that require an operator to take action.

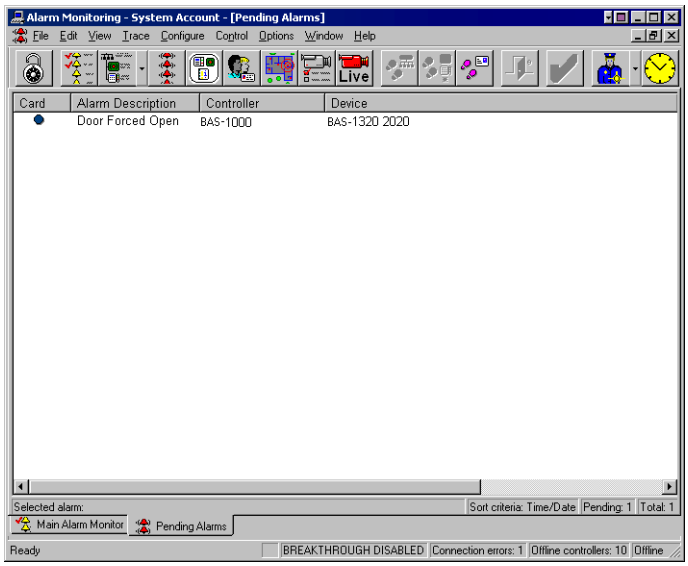
An initiating alarm is automatically deleted upon arrival of its corresponding canceling alarm. (e.g. Door Forced Open/Door Forced Open Cancelled).

If the Pending Alarms Window is left open, the window automatically updates itself. For example, when a pending alarm is acknowledged in the Main Alarm Monitoring window, it immediately ceases to display in the Pending Alarms window. If a pending alarm is an initiating alarm that becomes physically restored and must be acknowledged, it continues to display as a pending alarm until it is acknowledged. If a pending alarm is an initiating alarm that becomes physically restored but does not required acknowledgment, the alarm ceases to be a pending alarm.

Like the Main Alarm Monitoring window you can determine the type of information displayed about alarms through the **Configure** > **Columns** menu option. However, you cannot filter the type of alarms displayed through the **Configure** > **Alarm Filter** menu option. That is because the Pending Alarms window is intended to summarize ALL pending alarms.

Toolbar Shortcut

To display the window, select the **Pending Alarms** option from the **View** menu or click the View Pending Alarms toolbar button.



To view tables of the menu items and toolbar options, refer to Menus and Toolbars on page 33.

Procedure for Monitoring Alarms

Sort Alarms

Alarms are listed in the order indicated by the sort criterion. To determine the current sort criterion locate “Sort criteria” in the status bar (lower right side of the screen).

You can rearrange the order of existing and new alarms using either of these two methods:

- Clicking a column heading
- Selecting **View > Sort by** from the Main Alarm Monitoring menu.

The choices available in the **Sort by** submenu are:

Column name	Description
Alarm Description	Lists alarms alphabetically by alarm description.
Account Group	Lists alarms in order of receiver account group (panels). Receiver accounts are used to represent panels in a receiver setup.
Asset Name	List alarm alphabetically by asset name.
Asset Scan ID	Lists alarms in order of asset scan ID.
Associated Text	Indicates (Yes or blank) whether there is additional text associated with the alarm.
Badge Type	Displays the badge type associated with the alarm.
Biometric Score	Lists alarms in order of biometric score. A biometric score is based on how well a biometric access control reader matches a template in the database. By default, this sort option is not enabled. To enable this sort option, the “Biometric Score” column must first be added via the **Configure** > **Columns** menu option in Alarm Monitoring.
Card	Lists alarms numerically by the card number (badge ID), if the alarm is associated with a cardholder.
Controller	Lists alarms alphabetically by name of the controller with which the alarms are associated. The controller can be an access panel, fire panel, intercom exchange, receiver or receiver account.
Controller Time	Lists alarms in order of controller time. The time includes the hour and minute and the date includes the month, day and year. The display is based on the time zone setting selected in the Control Panel of your computer. Typically the display is adapted to the country in which you are located.
Device	Lists alarms alphabetically by name of the device (reader, alarm panel, intercom station etc.) associated with the alarm. If the alarm originates at a reader, the reader name displays. If the alarm originates at an alarm panel, the panel name displays.
Input/Output	Lists alarms alphabetically by name of the alarm input, if the alarm is generated at an alarm input.
Intercom Station Called	Lists alarms in order of intercom station called.

Column name	Description
Intrusion Area	Indicates the name of the area associated with the alarm. This is only displayed when the controller reported an area number along with the alarm.
Line Number	Displays alarms in order of line number.
Priority	Lists highest priority alarms at the top of the list, followed by medium priority alarms, with low priority alarms placed at the bottom of the list.
Time/Date	Lists alarms in chronological order. Within a given date (month, day and year) the alarms are sorted by time, which include hours and minutes and optionally seconds. • To view time in seconds go to the **Options** menu and select (place a checkmark beside) **Display Seconds**. • To view the most recent alarms at the bottom of the list, go to the **Options** menu and select (place a checkmark beside) **Ascending Time/Date**. To view the most recent alarms at the top of the list select (place a checkmark beside) **Descending Time/Date**.
Transmitter	Lists alarms in order of transmitter. *Transmitters* are devices that generate either an RF or IR (or both) signal that Visonic SpiderAlert receivers can receive. There are three types of transmitters: fixed, portable (hand-held) and man-down. For more information refer to the Personal Safety Devices Folder chapter in the System Administration User Guide.
Transmitter Input	Lists alarms in order of transmitter input.

For any sort, the second level sort criterion is always **Priority** and the third level criterion is always **Time/Date**. For example:

- If you sort by **Controller**, all alarms associated with the same controller will be sorted by **Priority** then by **Time/Date**.
- If you sort by **Priority**, all alarms with the same priority will be sorted by **Time/Date**.
- If you sort by **Time/Date**, alarms with the same time (to the second)/date will be sorted by **Priority**.

The sort criterion applies to the current window only. You can have one Main Alarm Monitoring window and various Trace windows, each with a different sort criterion. When you open a new Main Alarm Monitoring window, it is initially sorted by Priority.

Chapter 11: Acknowledge Alarms

Alarm Acknowledgment Window

Functions:

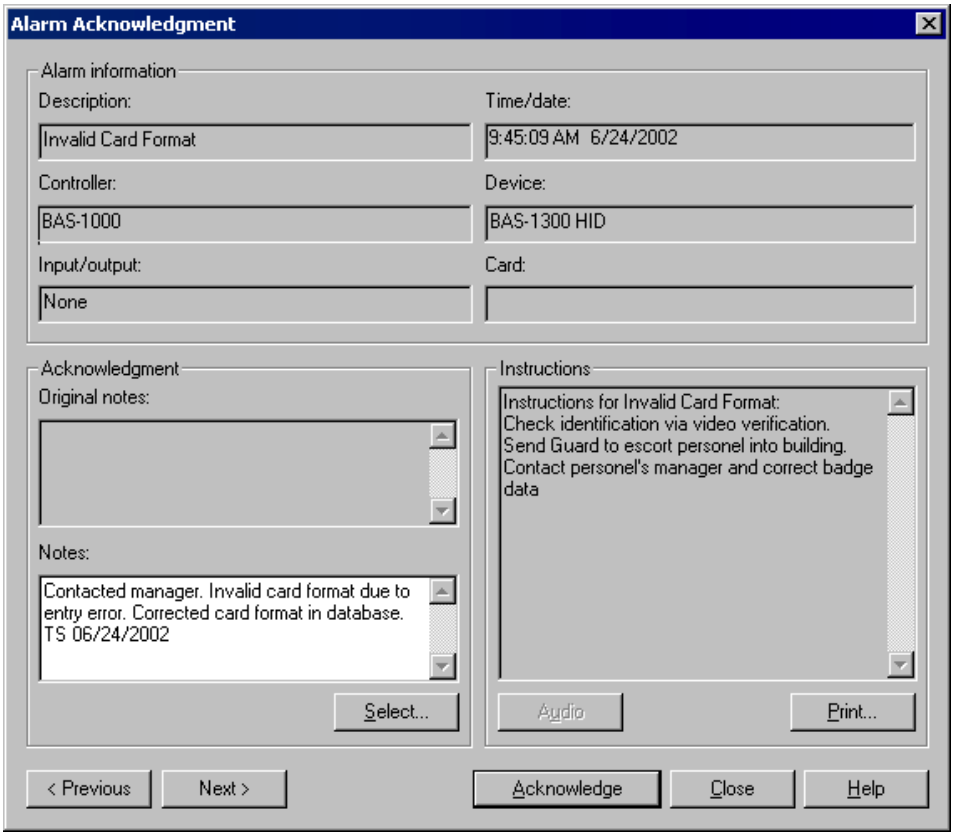
The Alarm Acknowledgment window enables you to:

- Respond (in the software) to an alarm.
- View or listen to stored instructions for a specific alarm.
- Print information pertaining to an alarm.
- Enter or select notes pertaining to an alarm.

Displayed by:

The Alarm Acknowledgment window can be displayed several ways:

- Double-click an alarm
- Highlight an alarm entry and from the **Edit** menu select **Acknowledge**
- Right-click an alarm entry and select **Acknowledge**



Alarm Acknowledgment Window

Form Element	Comment
Description	Contains the same name for the alarm as indicated in the Main Alarm Monitoring window.
Controller	Displays the name of the access panel associated with the alarm.
Input/output	If the alarm originated at an input/output device, displays the name of the device.
Time/date	Displays the time and date the alarm occurred.
Device	• If the alarm originated at a reader, displays the name of the reader. • If the alarm originated at an alarm panel, displays the name of the alarm panel.
Card	If the alarm is card-related, displays the cardholder name (if known*) and the badge ID. *Cardholder name would not be available for an “Invalid Badge” alarm, for example.
Original notes	Displays any notes carried forward from the associated original alarm.
Notes	Enables you to add your own comments/response to the selected alarm.
Select	Displays a window where pre-configured acknowledgment notes can be selected.
Instructions	Displays pre-configured instructions pertaining to the alarm.

Alarm Acknowledgment Window (Continued)

Form Element	Comment
Audio	Plays audio instructions.
Print	Prints the information from this window, including alarm information and any notes entered.
Previous	Displays information about the previous alarm in the Main Alarm Monitoring window.
Next	Displays information about the next alarm in the Main Alarm Monitoring window.
Acknowledge	Tells the B.A.S.I.S. software to acknowledge the currently selected alarm.
Close	Closes the Alarm Acknowledgment window.
Help	Displays online assistance for using this window.

Alarm Acknowledgment Procedures

An Action is any task performed by software as a result of an event or schedule.

When you acknowledge an alarm, you provide a software response to it. Your System Administrator can configure alarms so they have to or do not have to be acknowledged before they are deleted from the Main Alarm Monitoring window. Furthermore, your System Administrator can associate actions with an alarm so when the alarm is acknowledged an action or group of actions is automatically triggered.

Acknowledge an Alarm

1. Display the Alarm Acknowledgment window by double-clicking an alarm.
2. If the alarm has text instructions associated with it the information displays in the Instructions sub-window. Click [Print] to print the instructions.
3. If the alarm has voice instructions click [Audio].
4. To select pre-configured acknowledgment note(s) click [Select]. The Select Acknowledgment Notes dialog appears. Select the name of the pre-configured note and click [OK].
5. To add notes to the alarm, type your comments click in the **Notes** sub-window. If this is a canceling alarm, any notes carried forward from the associated initiating alarm display in the **Original Notes** field.
6. Click [Acknowledge] to acknowledge the alarm.
   - If your System Administrator has configured this alarm type for "Require Login On Ack." you must first log in before this alarm can be acknowledged.

An initiating alarm is an alarm that B.A.S.I.S. automatically deletes when the corresponding canceling alarm occurs.

   - If this is an initiating alarm, the corresponding canceling alarm may not be displayed until you acknowledge this alarm. Whether this happens depends upon how your system is set up.
   - Your System Administrator may have set up some types of alarms to be automatically deleted from the Main Alarm Monitoring window after you acknowledge them. If this is not the case, delete the alarm manually. For more information, refer to Delete an Alarm on page 121.
7. You can acknowledge multiple alarms without closing the Alarm Acknowledgment window. Repeat step 2 through 6 for each alarm you display in the Alarm Acknowledgment window. Use the navigation buttons to move through the list of alarms.
8. To close the Alarm Acknowledgment window, click [Close].

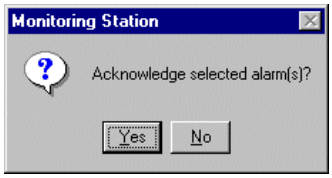
Fast/Group Acknowledge Alarms

The Fast/Group Acknowledge feature allows you to acknowledge a group of alarms simultaneously. This feature can be used without bringing up the acknowledgment dialog box.

1. Select the alarm(s) that you wish to acknowledge.
   - To choose two or more alarms, hold down the <Ctrl> key while selecting additional alarms.
   - To select all the alarms press <Ctrl> + <F11>.

Toolbar Shortcut

2. Acknowledge the group of alarms by completing one of the following:
   - Choose **Fast/Group Acknowledge** from the **Edit** menu
   - Right-click the selected group of alarms and choose **Fast/Group Acknowledge**
   - Click the Fast/Group Acknowledge toolbar button
   - Press <Ctrl> + <F12>
3. A message displays:



4. Click [Yes] to confirm the acknowledgment of the alarms.

Notes: If any of the chosen alarms require notes upon acknowledgment, you will be prompted to enter notes.

If any one of the alarms has already been acknowledged, it cannot be re-acknowledged. A message displays to inform you of how many alarms have been acknowledged. Click [OK] and delete the alarm(s).

The configuration for any given alarm may require that the operator log in upon acknowledging the alarm. If this is the case the user will be prompted to log in.

The configuration for an alarm may also require an acknowledgment password. If this is the case the operator will be prompted only once for the password (for each type of alarm).

Delete an Alarm

1. In the Main Alarm Monitoring window, highlight (click) the alarm you wish to delete.
2. Complete one of the following:
   - Press the <Delete> key.
   - From the **Edit** menu select **Delete**.
3. A confirmation message displays. Click [Yes].

Note: You can also right-click the alarm and select **Delete**. When the confirmation message displays click [Yes].

Delete All Alarms

Depending on how your System Administrator configured alarms, some alarms cannot be deleted until they have been acknowledged. B.A.S.I.S. will alert you if this is the case.

1. To delete all of the alarm entries from the current alarm view, select **Delete All** from the **Edit** menu.
2. A confirmation message displays. Click [Yes]. All entries will be removed from the Main Alarm Monitoring window.

Note: You can also delete multiple alarms in the Main Alarm Monitoring window using the <Shift> or <Ctrl> keys and right-clicking. Select the **Delete** option. A confirmation message displays. Click [Yes].

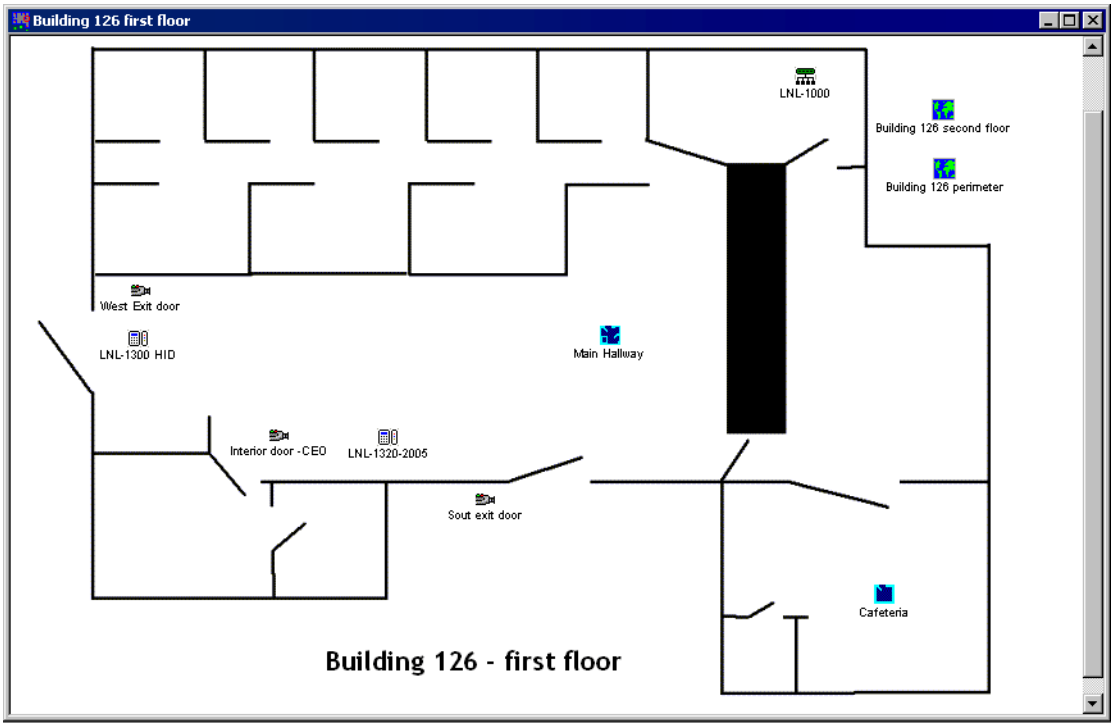
Display a Map

A *monitoring map* is a graphical representation of a facility or area monitored by the B.A.S.I.S. system. You can manually view maps associated with an alarm or you can set your display options to automatically display maps when an alarm occurs.

1. To manually display a map, open Alarm Monitoring.
2. If alarms are displayed in the Main Alarm Monitor window, right-click an alarm that has a map associated with it and select **View Map**. Otherwise, with the alarm selected choose **Map** from the **View** menu.
3. If no alarms are displayed in the Main Alarm Monitor window, select **Map Selection** from the **View** menu. Select the desired map and click [OK].

Note: If the selected device has multiple maps associated with it you will be prompted to select a map from a list provided. Do so and click [OK].

Example of a Map



Graphical symbols on the map indicate the location of devices. Using your mouse, scroll over each symbol to view the device status and any text associated with the device. For information on associating text with map icons refer to the MapDesigner User Guide.

Right-click a device symbol to perform a variety of operations depending on the type of device you select.

The word “ALARM” blinks, indicating an alarm’s location on the map.

- The blinking alarm displays only if there is one or more alarm designated as an “Active Alarm” in the System Administration software and if these alarms are unacknowledged/undeleted.

An alarm sprite is a small bitmap image used as an icon.

- The alarm sprite disappears once the alarm has been acknowledged.
- The alarm sprite disappears if the alarm has been deleted without acknowledgment (as in the case of an initiating alarm that is automatically replaced by a canceling alarm).
- The alarm sprite is not used for canceling alarms.

View Linked Maps

Several maps can be linked to each other using the MapDesigner software application. For more information refer to the “Place Icons on a background” section in the MapDesigner User Guide.

To view linked maps do one of the following:

- If the map that is currently displayed has a link to another map, you can double-click the icon or right-click and select **Switch Map**.
- With a map currently displayed, click the map icon beside the **File** menu option. If you have previously brought up more than one map, a **Back 1 Map** menu option displays. If you go back one map, a **Forward 1 Map** menu option displays.

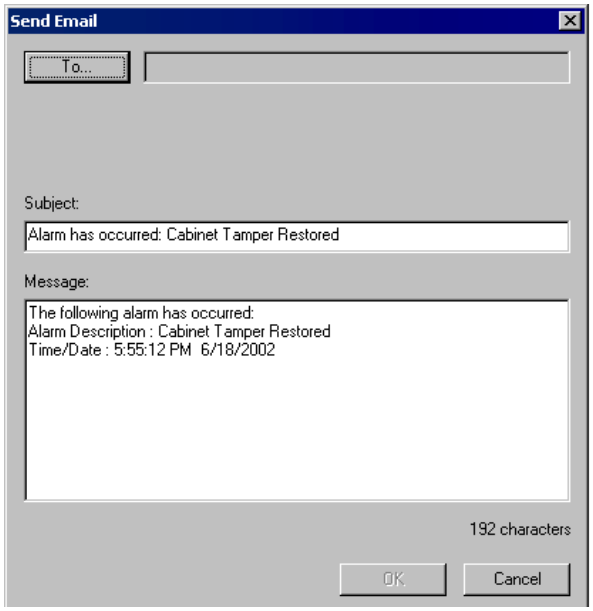
- From the **View** menu select Map Selection. Highlight a new map and click [OK].

Send an E-mail

Using B.A.S.I.S. software you can automatically or manually send electronic mail with alarm information. Contact your System Administrator to automatically send electronic mail for specific alarms.

To manually send an e-mail using Alarm Monitoring:

1. Verify the Global Output Server is running by clicking Start and selecting **Programs** > **B.A.S.I.S. ET**> **Global Output Server**.
2. Right-click an alarm and select **Send Email**. The Send Email window opens.
3. Click [To] and select (place a checkmark beside) the desired e-mail addresses. Use the <Ctrl> or the <Shift> key to select multiple addresses.
4. The subject and body of the message are automatically populated with information that describes the alarm. Click in either field to make any changes.
5. Click [OK].

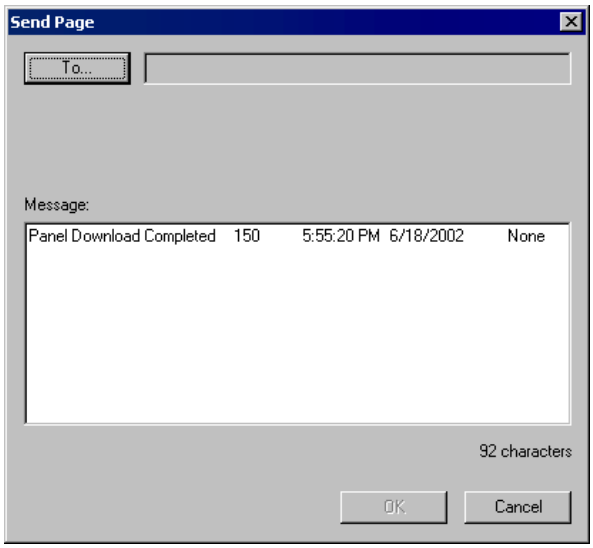


Field/button	Description
To	Allows you to select an e-mail address that is already in the database.
Subject	Displays the subject of the message. By default, the description of the alarm that has occurred is displayed. To change it, type over the text.
Message	Displays the body of the message being sent. By default, information pertaining to the alarm is displayed. To change it, type over the text.
OK	Once you are done, click the [OK] button to send the message and exit the window.
Cancel	To exit the window without sending an e-mail message, click the [Cancel] button.

Send a Page

Using B.A.S.I.S. software you can send a page to a recipient with alarm information.

1. Verify the Global Output Server is running by clicking Start and selecting **Programs** > **B.A.S.I.S. ET** > **Global Output Server**.
2. Right-click an alarm and select **Send Page**. The Send Page window opens.
3. Click [To] and select (place a checkmark beside) the pager number of the recipient.
4. The message field is automatically populated with an alarm description, the time and date on which it occurred and the location (which reader/alarm panel).
5. Click [OK] to send the page.



Field/Button	Description
To	Allows you to select pager number that is already in the database.
Message	Displays the body of the message being sent. By default, information pertaining to the alarm is displayed. To change it, type over the text.
OK	Once you are done, click the [OK] button to send the message and exit the window.
Cancel	To exit the window without sending a page, click the [Cancel] button.

Advanced Operator Procedures

Chapter 12: Cardholders Folder

The Cardholders folder contains forms with which you can:

- Add, modify and delete cardholder and visitor records.
- Assign cardholders or groups of cardholders to different segments.
- Create badge records for cardholders and visitors.
- Assign access levels to active badges for cardholders and visitors.
- Assign one or more Precision Access groups to a badge (if Precision Access is used on your system).
- Search for and display cardholders and visitors biometrics records.
- Search for cardholders and visitors visit records.
- Assign and track assets to cardholders and visitors.
- Link directory accounts to cardholders and visitors.
- Assign a cardholder as a tour guard.
- Assign security clearance levels to tour guards.
- Create and print reports containing cardholder information.

The folder contains up to eleven forms: the Cardholder/Visitor form, the Badge form, the Segments form (if segmentation is enabled), the Access Levels form, the Precision Access form (if in use), the Biometrics form, the Visits form, the Assets form, the Directory Accounts form, the Guard Tours form and the Reports form.

Toolbar Shortcut

The Cardholders folder is displayed by selecting the **Badge Info** choice from the **View** menu, or by selecting the Cardholders toolbar button.

Cardholders Folder Overview

The forms in the Cardholders folder are visually divided into four sections; the right section, the upper-left section, the middle-left section and the bottom section.

Several of the form elements in these sections are common to every form in the cardholders folder. Refer to the following table for descriptions of the common form elements.

Notes: This documentation refers to cardholder data fields that are shipped as the default by Best. If you have used the FormsDesigner application to

customize your cardholder data, the elements on your cardholders folders forms will be different.

The Segments form is only available if segmentation is enabled on your system

The availability of certain forms and fields in the Cardholders folder is subject to licensing restrictions.

Cardholders Folder

Form Element	Type	Comment
Common form elements - right section		
Photo display	display	Displays the cardholder's photo as it appears on their badge.
Signature display	display	Displays the cardholder's signature as it appears on their badge.
Last access	display	If **Show Last Granted Location** is selected in the **Cardholder** menu, displays information about the most recent valid access by this cardholder, including the triggered event, date, time and reader name. If **Show Last Attempted Location** is selected in the **Cardholder** menu, displays information about the most recent access attempt (whether access was granted or not) by this cardholder, including the triggered event, date, time and reader name.
Badge ID	display	Displays the numeric identifier assigned to the cardholder's active badge.
Issue code	display	Displays the issue code assigned to the cardholder's active badge.
Prints	display	Displays the number of times the active badge has been printed.
Activate	display	Displays the date when the badge becomes valid.
Deactivate	display	Displays the date when the badge becomes invalid.
Common form elements - upper-left section		
Last name	text	Indicates the cardholder's last name.
First name	text	Indicated the cardholder's first name.
Middle name	text	Indicates the cardholder's middle name.
Cardholder ID	numeric	Indicates the cardholder's ID number. **Note:** This field is not displayed on the Visitor form.
Badge type	drop-down list	Indicates the cardholder's badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.
Common form elements - bottom section		
Search	push button	Displayed in view mode on every form in the Cardholders folder. This button is used to search for existing cardholder records.

Cardholders Folder (Continued)

Form Element	Type	Comment
Add	push button	Enabled in view mode on the Cardholder/Visitor and Badge form and is used to add a record. **Note:** This button is displayed but not enabled on the Segments form, the Access Levels form, the Precision Access form, the Biometrics form, the Visits form, the Guard Tours form and the Reports form because these records are not added in the Cardholders folder.
Modify	push button	Displayed in view mode on every form in the Cardholders folder. **Note:** This button will be displayed but will not be enabled on the Directory Accounts form and the Reports form, because directory account and report records cannot be modified.
Delete	push button	Enabled in view mode on the Cardholder/Visitor and Badge form and is used to delete a record. **Note:** This button is displayed but not enabled on the Segments form, the Access Levels form, the Precision Access form, the Biometrics form, the Guard Tours form and the Reports form because these records are not deleted in the Cardholders folder.
Print	push button	Displayed in view mode on every form in the Cardholders folder. When selected, displays the **Badge Printing** window from where you can print the active badge for the current record, or the active badges for all records found in a search. You can also log and print errors encountered during the print operation. **Note:** When you select this button on the Reports form, the **Print Report Options** window is displayed. For more information, refer to Chapter 17: Print Report Options Window on page 297.
Encode	push button	**Note:** Displayed in view mode on every form in the Cardholders folder. When selected, displays the **Encode Badge** window from where you can encode the badge configurations selected for the cardholder onto a smart card. For more information refer to the Card Formats Folder chapter in the System Administration User Guide.For cardholder records with guest badge types, clicking this button will display the Increment Issue Code window. The availability of this button is subject to licensing restrictions.
	push button	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the first record that matches your search criteria.

Cardholders Folder (Continued)

Form Element	Type	Comment
	push button	Displayed in search mode on every form in the Cardholders folder. When selected, by default moves 10 matching records back. You can change the number of records moved back by modifying the value in the **Number of records to scroll for fast forward and rewind** field on the **View Options** window. The View Options window is displayed by selecting **View Options** from the **Cardholder** menu.
	push button	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the previous record that matches your search criteria.
	push button	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the next record that matches your search criteria.
	push button	Displayed in search mode on every form in the Cardholders folder. When selected, by default moves 10 matching records forward. You can change the number of records moved forward by modifying the value in the **Number of records to scroll for fast forward and rewind** field on the **View Options** window. The View Options window is displayed by selecting **View Options** from the **Cardholder** menu.
	push button	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the last record that matches your search criteria.
OK	push button	Displayed in search or modify mode on every form in the Cardholders folder. When selected, saves the changes made to the current record, or begins the requested search.
Cancel	push button	Displayed in search or modify mode on every form in the Cardholders folder. When selected, cancels the pending requested action.
Clear	push button	Displayed in search or modify mode on every form in the Cardholders folder. When selected, clears all current record information that can be cleared from the current form.
Clear All	push button	Displayed in search or modify mode on every form in the Cardholders folder. When selected, clears all current record information that can be cleared from *all* forms in the folder.
Capture	push button	Displayed in add or modify mode on the Cardholder/Visitor form, the Segments form, the Badge form, the Access Levels form, the Precision Access form and the Biometrics form. Displayed in modify mode on the Visits form. When selected, opens the Multimedia Capture module. **Note:** The availability of the Multimedia Capture module is subject to licensing restrictions.
Last Search	push button	Displayed in search mode on every form in the Cardholders folder. When selected, retrieves the same group of records that was found by the most recent search operation.

Cardholders Folder (Continued)

Form Element	Type	Comment
Record count	numeric	Displayed in view mode on every form in the Cardholders folder and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Person type	drop-down list	In search mode, select the type of record you want to search. Choices are: • All - when selected, your search will locate both Cardholder and Visitor records • Cardholders - when selected, your search will only locate cardholder records • Visitors - when selected, your search will only locate visitor records

Cardholders Folder Procedures

The following procedures pertain to every form in the Cardholders folder unless otherwise noted.

Cardholder Search Capabilities

In search mode, you can search on any combination of fields in the Cardholders folder, including the Cardholder, Badge and Access Levels forms.

Comparison Operators

For text fields such as **Last name** and **First name**, the default comparison is "begins with". The search results will include any records whose values begin with the characters that were entered. For example, when searching by last name, a filter of 'L' will find 'Lake', 'Lewis', etc. A filter of 'Lake' will find 'Lake', 'Lakeland', etc.

For all other field types, such as drop-down lists and numeric fields, the default comparison is "equal to". For example, searching on the **Badge ID** field with a value of "123" will find the cardholder whose badge ID is equal to 123.

In addition to the default comparison, you can customize your search by prefixing the search text with a comparison operator. The supported operators are:

Comparison operator	Description
=	Equal to (can be used to force an equals comparison for text fields)
!= or <>	Not equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to

For drop-down lists, only the “not equal to” operator is supported in addition to the default “equals” comparison. To perform a “not equal to” comparison for a drop-down list, first select the value from the list, then type “<>” in front of the text.

Search Text Fields for “Contains”

In addition to the default “begins with” searching for text fields, you can do a search for “contains” by prefixing the text with a percent sign (“%”). For example, typing “%mit” in the **Last name** field will find all people whose last name contains the text “mit”.

Search for Empty Values

You can search for cardholder records that have an “empty” value for a field by typing an equal sign (“=”) in the field and nothing else. For example, typing an “=” in the **Department** field will find all people that do not have a department assigned.

Search on Multiple Fields

When you search on multiple fields, the criteria is combined with “and”. For example, typing “A” in **Last name** field and “B” in **First name** field will find all people whose last name begins with “A” *and* whose first name beings with “B”. One exception is searching on access levels, which uses an “or” comparison for multiple selections in that field. For example, selecting both “Access Level A” and “Access Level B” will find all cardholders with either “Access Level A” *or* “Access Level B” assigned.

For fields that have multiple representations on a form, you can search on a range of values. For example, the **Badge ID** field can be found on both the middle-left section of the Badge form and the right section of the Badge form. This allows you to search for badge ID ranges. For example, you can type “>= 100” in one field and “<= 200” in the other to find all badges with IDs between 100 and 200 (inclusive).

Search for a Cardholder Record

1. From the **View** menu select **Badge Info**.
2. Click [Search].
3. From the **Person type** drop-down list (located in the lower right portion of the screen) select the type of record you want to search. Choices are:
   - All - when selected, your search will locate both Cardholder and Visitor records
   - Cardholders - when selected, your search will only locate cardholder records
   - Visitors - when selected, your search will only locate visitor records

Note: The **Person type** drop-down list is subject to licensing restrictions. If this field is not displayed, move on to the next step.

4. Specify your search criteria by typing full or partial entries in the enabled fields.
5. Click [OK].

   B.A.S.I.S. retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

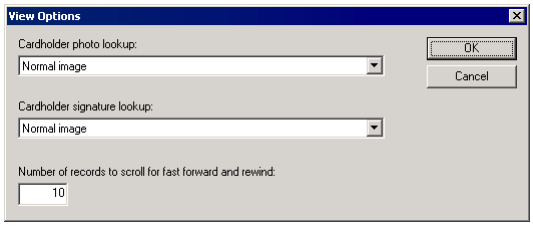
Retrieve the Most Recent Search Results

1. Click [Search].
2. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
3. If you want, modify your search criteria.
4. Click [OK].

   B.A.S.I.S. retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

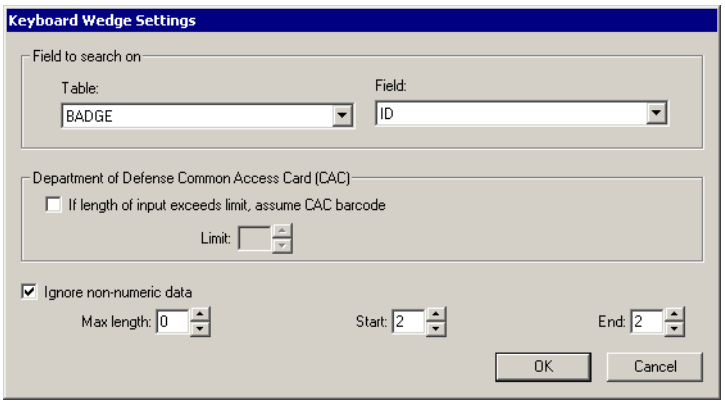
Change the Cardholders Folder View Options

1. Select **View Options** from the Cardholder menu. The **View Options** window opens.



2. From the **Cardholder photo lookup** drop-down list, select the image type you want displayed in **Photo** display (located in the right section of the Cardholders folder forms).
   Choices include:
   - None - no image will be displayed
   - Normal image - a photo image will be displayed as it was originally captured
   - Normal image with chromakey - a photo image will be displayed, but without its background
3. From the **Cardholder signature lookup** drop-down list, select the type of signature you want displayed in **Signature** display (located in the right section of the Cardholders folder forms).
   Choices include:
   - None - no signature will be displayed
   - Normal image - a signature will be displayed
4. In the **Number of records to scroll for fast forward and rewind** field, type in the number of records you want to move backwards and forwards when you select the and push buttons.
5. Click [OK].

Keyboard Wedge Settings Window



A wedge scanner, also sometimes referred to as a wedge reader, is a device that is attached to a keyboard and used to scan badge IDs as direct keyboard input. Wedge scanners can be used with B.A.S.I.S. to:

- **Add a badge.** In this scenario, each card entry station has a wedge scanner. The operator clicks [Add] and swipes the badge with the wedge scanner to read the badge ID. This is equivalent to typing in the badge ID at the keyboard. When a wedge scanner is used in this manner, no configuration of the settings on the Keyboard Wedge Settings window is needed.
- **Search for a badge.** The normal way to search for a badge in B.A.S.I.S. is to click [Search] and then specify what to search for, such as badge ID or social security number. When a wedge scanner is used, the [Search] button does not need to be clicked; instead, the system specifically searches on one predefined criteria. When a wedge scanner is used in this manner, the settings on the Keyboard Wedge Settings window must be properly configured.

When to Use the Keyboard Wedge Settings Window

The Keyboard Wedge Settings window only needs to be configured on systems that will be using a wedge scanner to search for badges. This may include:

- **MobileVerify stations.** MobileVerify stations typically use a wedge scanner because using a keyboard on a mobile computer is awkward. The wedge scanner provides a quick way to search for a cardholder and instantly grant or deny access based on the system's recommendation.
- **Enterprise installations.** Some Enterprise installations may choose to use a wedge scanner as a way of preventing duplicate badges. Since the card is swiped instead of typing a number in, the possibility of entering a wrong badge ID is eliminated.

The settings on the Keyboard Wedge Settings window determine the format of the data that is sent between a wedge scanner and the B.A.S.I.S. system, and are specified on a per workstation basis. Administrative rights to the workstation are required to change these settings because any changes must be written to the **ACS.INI** file.

Displaying the Keyboard Wedge Settings Window

The Keyboard Wedge Settings window is displayed by selecting **Keyboard Wedge Settings** from the **Cardholder** menu. (In System Administration, ID CredentialCenter, Visitor Management, and View/Edit Only the **Cardholder** menu is only displayed after selecting **Cardholders** from the **Administration** menu. In Alarm Monitoring and Digital Video, the **Cardholder** menu is displayed after clicking the toolbar button.)

CAC Barcodes

A common access card (CAC) is a military-issued ID card that is issued to active duty personnel, selected reservists, Department of Defense civilian employees, eligible contractors, and some foreign nationals. Retirees, family members, and inactive reservists are not currently issued a CAC card.

Configuring B.A.S.I.S. to Read CAC Barcodes

To set the B.A.S.I.S. system up to read CAC cards, the **If length of input exceeds limit, assume CAC barcode** checkbox on the Keyboard Wedge Settings window must be selected. A limit also needs to be specified. If only CAC cards will be read, then the **Limit** can be set to 0. However, most systems will also need to have the ability to read other cards in addition to CACs, so the limit will need to be set to an appropriate value.

For example, a military base that assigns badge IDs to the people on its base may want to be able to read those badge IDs as well as CACs because visitors from other bases will only have a CAC. In this case, the limit would need to be set to an appropriate number. If the badge IDs were all nine digits long, then an appropriate limit would be ten because CAC barcodes are much longer than ten digits.

Scanning Barcodes with a Wedge Scanner

When an ID is scanned, B.A.S.I.S. determines the length of the number that was scanned. If the number of digits exceeds the limit, then the number is treated as a CAC number, and the social security number is decrypted and searched up.

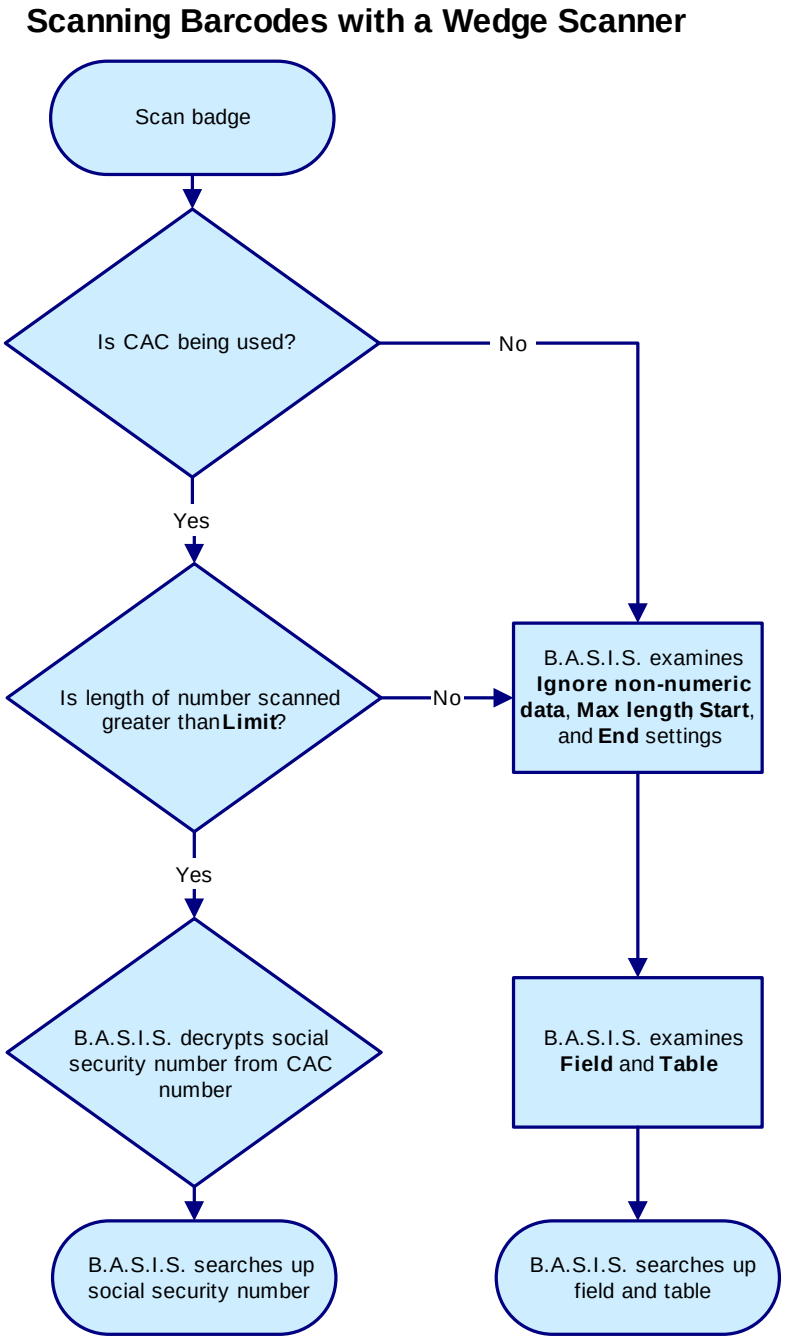
If the number of digits is less than the limit, then the maximum length, start, and end settings are applied to the string and used to extract the search criteria (typically badge ID or social security number).

After those settings are examined, the system then examines the **Table** and **Field** and searches that information up. The **Table** and **Field** specified depend on what information is encoded on the card that will be read in addition to the CAC. Common options include:

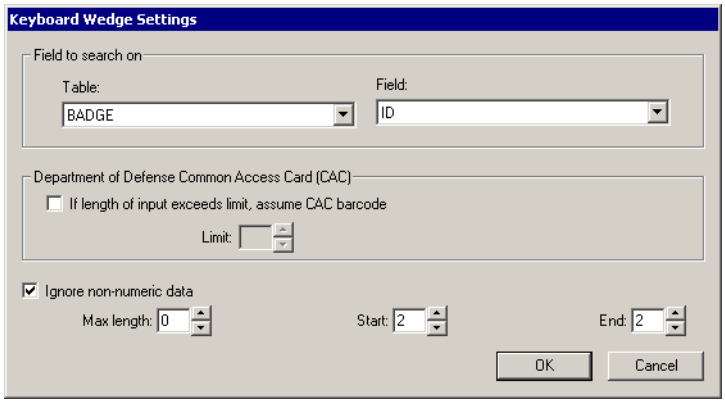
- **Badge ID**. If searching on Badge IDs, select the BADGE table and the ID field.
- **Social security number**. If searching on social security numbers, select the EMP table and the SSNO field.

- **User-defined field.** If searching on a user-defined field, select the desired table and field. For example, a company may wish to search on a table and field that is unique to their system, such as an employee number.

The following flowchart describes what happens when a barcode is scanned with a wedge scanner:


Scanning Barcodes with a Wedge Scanner
Scan badge
Is CAC being used?
No
Yes
Is length of number scanned greater than **Limit**?
No
B.A.S.I.S. examines **Ignore non-numeric data**, **Max length**, **Start**, and **End** settings
Yes
B.A.S.I.S. decrypts social security number from CAC number
B.A.S.I.S. examines **Field** and **Table**
B.A.S.I.S. searches up social security number
B.A.S.I.S. searches up field and table

Keyboard Wedge Settings Window



Keyboard Wedge Settings Window

Form Element	Type	Comment
Table	drop-down list	Select the table in the B.A.S.I.S. database that you wish to search on when keyboard input is detected. If searching for badge ID numbers, select the BADGE table, and if searching for social security numbers, select the EMP table. **Note:** If CAC is being used and an ID is scanned that has more than the specified **Limit** of digits, then the **Table** and **Field** will be ignored.
Field	drop-down list	Select the field in the selected table in the B.A.S.I.S. database that you wish to search on when keyboard input is detected. If searching for badge ID numbers, select ID (in the BADGE table), and if searching for social security number, select SSNO (in the EMP table). **Note:** If CAC is being used and an ID is scanned that has more than the specified **Limit** of digits, then the **Table** and **Field** will be ignored.
If length of input exceeds limit, assume CAC barcode	checkbox	If selected, CAC (Common Access Card) barcodes can be used. This allows military code 3of9 barcodes to be scanned and decoded into the cardholder's social security number. If you do not wish to use this feature, leave this checkbox deselected. If this checkbox is selected, you must specify an appropriate **Limit**. When this checkbox is selected and an ID is scanned, the number of digits will be examined. • If the number of digits is less than or equal to the **Limit**, then the system will search on the **Table** and **Field**. • If the number of digits is greater than the **Limit**, then the system will assume the ID was a CAC, decrypt the social security number, and search the social security number up.

Keyboard Wedge Settings Window (Continued)

Form Element	Type	Comment
Limit	numeric/spin buttons	The **Limit** field is only enabled when the **If length of input exceeds limit, assume CAC barcode** checkbox is selected. If the **Limit** is set to zero, then only CAC can be read. Setting a limit greater than zero enables the system to recognize two different formats. When an ID is scanned, the number of digits will be examined. • If the number of digits is less than or equal to the **Limit**, then the system will search on the **Table** and **Field** using the **Max length**, **Start**, and **End** settings. • If the number of digits is greater than the **Limit**, then the system will assume the ID was a CAC, decrypt the social security number, and search the social security number up.
Ignore non-numeric data	checkbox	If selected, non-numeric data is removed and not counted as a placeholder. This is important for scans that include dashes in the social security number. For example, if an ID is scanned that has 123-45-6789 encoded, the system will search for 123456789.
Max length	numeric/spin buttons	A maximum length must be provided if the wedge scanner does not automatically provide a line feed carriage return. This allows the wedge scanner to be used as long as the length of the scan is always the same (i.e., social security number). If 0 or -1 is specified, then the whole string will be read in.
Start	numeric/spin buttons	The **Start** field works in combination with the **End** field. When an ID is scanned, a string of numbers are read. As long as the ID is not a CAC, that string of numbers typically contains the actual badge ID or social security number. For a CAC, that string of numbers doesn't contain the actual social security number, but B.A.S.I.S. does "decrypt" the social security number from the string. The **Start** position is important because the string of numbers may contain other numbers in addition to what is being searched for; it is the first position in the string of numbers that contains a digit of what is being searched for. The **End** position is the last digit of what is being searched for. The **End** position should be greater than or equal to the **Start** position. Take for example the string 123456789. If 4 is the **Start** position and 7 is the **End** position, then the B.A.S.I.S. system will search on 4567. If you specify an **End** position that is less than the **Start** position, B.A.S.I.S. assumes the end is 255. Therefore, for the string 123456789 with 4 as the **Start** and 3 as the **End**, B.A.S.I.S. would search on 456789.

Keyboard Wedge Settings Window (Continued)

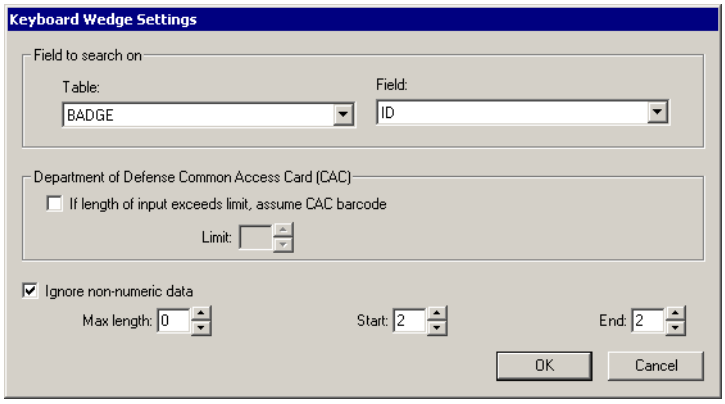
Form Element	Type	Comment
End	numeric/spin buttons	The **End** field works in combination with the **Start** field. As long as the ID is not a CAC, that string of numbers typically contains the actual badge ID or social security number. For a CAC, that string of numbers doesn't contain the actual social security number, but B.A.S.I.S. does "decrypt" the social security number from the string. The **Start** position is important because the string of numbers may contain other numbers in addition to what is being searched for; it is the first position in the string of numbers that contains a digit of what is being searched for. The **End** position is the last digit of what is being searched for. The **End** position must be greater than or equal to the **Start** position. Take for example the string 123456789. If 4 is the **Start** position and 7 is the **End** position, then the B.A.S.I.S. system will search on 4567. If you specify an **End** position that is less than the **Start** position, B.A.S.I.S. assumes the end is 255. Therefore, for the string 123456789 with 4 as the **Start** and 3 as the **End**, B.A.S.I.S. would search on 456789.
OK	push button	Applies the selected wedge scanner settings and closes the Keyboard Wedge Settings window.
Cancel	push button	Closes the Keyboard Wedge Settings window without applying any changes made.

Keyboard Wedge Settings Window Procedures

Configure a Wedge Scanner

How the B.A.S.I.S. system interprets the information it receives from a wedge scanner can be configured by doing the following:

1. In System Administration, ID CredentialCenter, Visitor Management, or View/Edit Only, select **Cardholders** from the **Administration** menu. In Alarm Monitoring and Digital Video, click the toolbar button.
2. Select **Keyboard Wedge Settings** from the **Cardholder** menu.
3. The Keyboard Wedge Settings window opens.



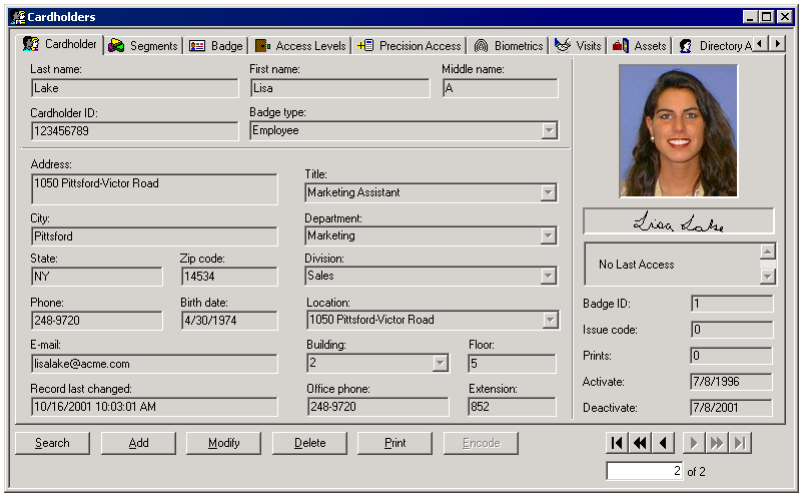
   a. Specify the **Table** and **Field** you wish to search on when non-CAC input is detected. By default, the system searches on the ID field in the BADGE table. If for example you wanted to search based on social security number instead of badge ID, you would select the SSNO field in the EMP table.
   b. If CAC (Common Access Card) barcodes will be used, select the **If length of input exceeds limit, assume CAC barcode** checkbox and specify the limit. This allows military code 3of9 barcodes to be scanned and decoded into the cardholder's social security number. If you do not wish to use this feature, leave this checkbox deselected.
   c. Select whether to ignore non-numeric data. By default, the **Ignore non-numeric data** checkbox is selected. This is important for scans that include dashes in the social security number.
   d. Specify the maximum length in the **Max length** field. A maximum length must be provided if the wedge scanner does not automatically provide a line feed carriage return. This allows the wedge scanner to be used as long as the length of the scan is always the same (i.e., social security number).

Note: If 0 or -1 is specified, then the whole string will be read in.

e. Specify the start and end. In a string of numbers that contains a search criteria (typically social security number or badge ID), start and end are the first and last position, respectively, that contain the search criteria.

f. Click [OK].

Cardholder Form



Cardholder Form Overview

In the System Administration and ID CredentialCenter applications, the Cardholder form is used to:

- Define a cardholder.
- Enter social security number, birth date, address and other demographic information into the cardholder record.
- Choose a badge type for the cardholder.
- Access the Multimedia Capture Module (subject to licensing restrictions).

In the Visitor Management application, the Cardholder form is used to search for a cardholder.

Cardholders Folder - Cardholder Form

Form Element	Type	Comment
Cardholder data	text/drop-down lists/numeric	Displayed in view mode. When adding or modifying a cardholder record, enter the cardholder's information such as name, address and department into these fields.
Record last changed	numeric	Displayed in view mode and indicates the date on which the selected cardholder record was last modified and saved. This date is updated only when cardholder information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Cardholder Form Procedures

Add a Cardholder Record

1. Select the **Badge Info** choice from the **View** menu. The Cardholders folder opens. By default, the Cardholder form is displayed.
2. Click [Add].
3. From the **Person type** drop-down list, select **Cardholders**.

Note: The **Person type** drop-down list is subject to licensing restrictions. If this field is not displayed, move on to the next step.

4. Enter the cardholder's name and any additional information in the cardholder data fields.

Note: You can switch to other tabs and modify the other forms at this time.

5. If you want to add a photograph or signature to the cardholder record, click [Capture]. The Multimedia Capture module opens. For more information refer to the Multimedia Capture Module appendix in the System Administration User Guide.
6. Click [OK] to save the record.

Modify a Cardholder Record

1. Locate the cardholder record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Cardholder Record

1. Locate the cardholder record you want to delete.
2. Click [Delete].
3. Click [OK].

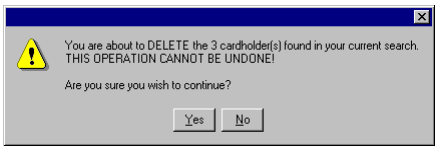
Note: If you delete the cardholder record, all associated records (Badge, Access Levels, Precision Access, Biometrics, Assets, Directory Accounts, Guard Tours and Visits) for the cardholder are also removed from the database.

Delete a Selected Group of Cardholder Records

Warning

This is a powerful feature that cannot be undone. Use caution when performing a bulk deletion of cardholders to ensure that you only delete the cardholders you want to eliminate from your database.

1. Locate the cardholder records you want to delete using the search function. The bulk delete operation will act on **all** cardholders that result from the current search.
2. Select **Bulk** > **Delete Cardholders in Search** from the **Cardholder** menu. The following message is displayed:


You are about to DELETE the 3 cardholder(s) found in your current search.
THIS OPERATION CANNOT BE UNDONE!
Are you sure you wish to continue?
Yes
No

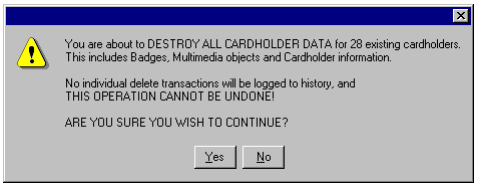
3. Click [Yes].

Destroy all Cardholder Data

Warning

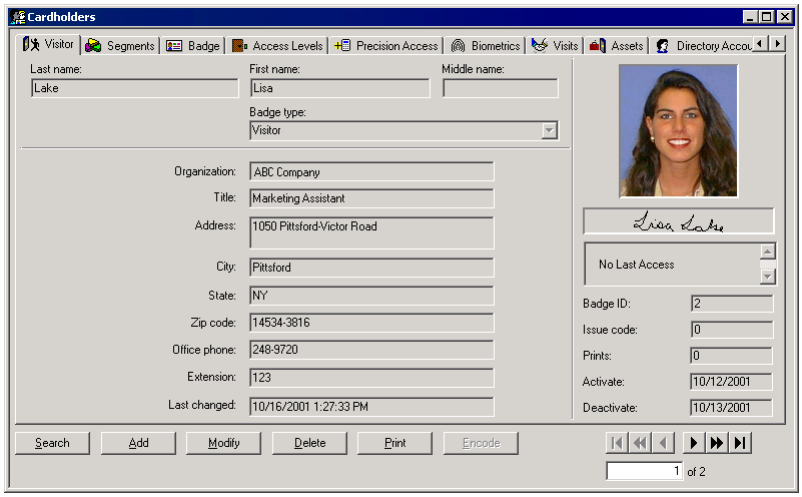
This feature will wipe out all cardholder and badge information from the database without any transaction logging and cannot be undone. This function is mainly intended for wiping out data after a system has been installed and tested. For example, when you are first setting up the system and have imported cardholder data but you wish to change and redo the import. This function provides a quick way to wipe out all existing cardholder data.

1. Select **Bulk** > **Destroy ALL Cardholder Data** from the **Cardholder** menu. The following message is displayed:


You are about to DESTROY ALL CARDHOLDER DATA for 28 existing cardholders.
This includes Badges, Multimedia objects and Cardholder information.
No individual delete transactions will be logged to history, and
THIS OPERATION CANNOT BE UNDONE!
ARE YOU SURE YOU WISH TO CONTINUE?
Yes
No

2. Click [Yes] to confirm the deletion of all cardholder data.

Visitor Form



Visitor Form Overview

To provide integration with Visitor Management, visitor records can be searched and viewed in the Cardholders folder. When the current record is a visitor, the first tab in the window changes from Cardholder to Visitor and will display the appropriate fields.

If you select the [Add] button on the Cardholder form, or the [Search] button on any of the forms in the Cardholders folder, the **Person type** drop-down list is displayed in the bottom section of the form.

The drop-down list choices are:

- All - when selected, your search will locate both Cardholder and Visitor records
- Cardholders - when selected, your search will only locate cardholder records
- Visitors - when selected, your search will only locate visitor records

Notes: With the exception of the **Allowed visitors** checkbox and the [Capture] button (in modify mode only) on the Visits form, visit records cannot be added, modified, or deleted from the Cardholders folder. To add, modify, or delete visits, you must purchase the Visitor Management module.

The availability of this form is subject to licensing restrictions.

Cardholders Folder - Visitor Form

Form Element	Type	Comment
Visitor data	text/drop-down lists/numeric	Displayed in view mode. When adding or modifying a visitor record, enter the visitor's information such as name, address and organization into these fields.
Last changed	numeric	Displayed in view mode and indicates the date on which the selected visitor record was last modified and saved. This date is updated only when visitor information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Visitor Form Procedures

Add a Visitor Record

1. Select the **Badge Info** from the **View** menu.The Cardholders folder opens. By default, the Cardholder form is displayed.
2. Click [Add].
3. From the **Person type** drop-down list, select **Visitors**.
4. Enter the visitor's name and any additional information in the visitor data fields.

Note: You can switch to other tabs and modify the other forms at this time.

5. If you want to add a photograph or signature to the visitor record, click [Capture]. The Multimedia Capture module opens. For more information

refer to the Multimedia Capture Module appendix in the System Administration User Guide.

6. Click [OK] to save the record.

Modify a Visitor Record

1. Locate the visitor record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] button to save the changes, or the [Cancel] button to revert to the previously saved values.

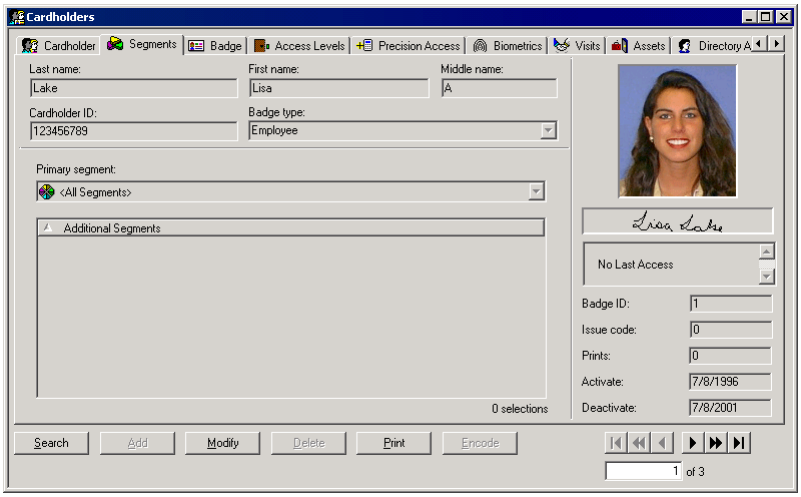
Delete a Visitor Record

1. Locate the visitor record you want to delete.
2. Click [Delete].
3. Click [OK].

Note: If you delete the visitor record, all associated records (Badge, Access Levels, Precision Access, Biometrics, Assets, Directory Accounts, Guard Tours and Visits) for the visitor are also removed from the database.

Segments Form

Note: The Segments tab is only displayed if segmentation is enabled on your system.



Segments Form Overview

The Segments form is used to:

- Modify a cardholder's segment assignment.
- Change a group of cardholder's segments.

Cardholders Folder - Segments Form

Form Element	Type	Comment
Primary segment	drop-down list	In modify mode, select which primary segment you want the selected cardholder to be assigned to. A cardholder can be assigned to a primary segment and as well as additional segments.
Additional Segments listing window	display	Lists all of the segments that have been configured in the system. For more information refer to the Segments Folder chapter in the System Administration User Guide.
Number of selections	display	Displays the number of segments that have been selected in the **Additional Segments** listing window. For example: 2 selections.

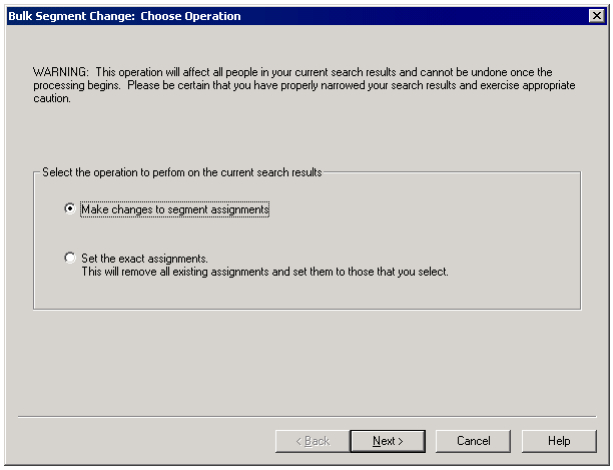
Segments Form Procedures

Modify a Cardholder's Segment Assignment

1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Segments tab.
3. Locate the cardholder record that you want to modify.
4. Click [Modify].
5. From the **Primary segment** drop-down list, select which primary segment you want the selected cardholder to be assigned to.
6. If you want to assign additional segments (if any exist), click on an entry in the **Additional Segments** listing window to select it. You can select multiple entries.
7. Click [OK].

Modify a Group of Cardholder's Segments

1. Locate the group of cardholder records you want to change.
2. Select **Bulk** > **Change Cardholder Segments** from the **Cardholder** menu. The **Bulk Segment Change** window opens.

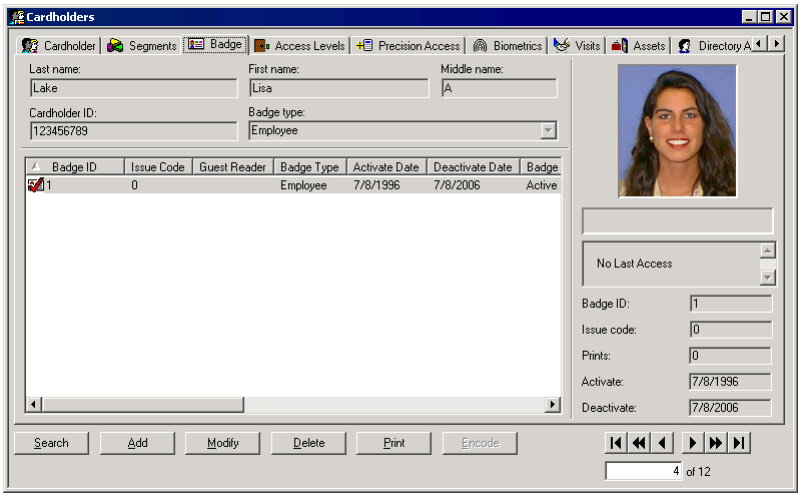

Bulk Segment Change: Choose Operation
WARNING: This operation will affect all people in your current search results and cannot be undone once the processing begins. Please be certain that you have properly narrowed your search results and exercise appropriate caution.
Select the operation to perfom on the current search results
Make changes to segment assignments
Set the exact assignments.
This will remove all existing assignments and set them to those that you select.
< Back
Next >
Cancel
Help

3. Select the **Make changes to segment assignments** radio button or select the **Set the exact assignments** radio button if you want all assignments that

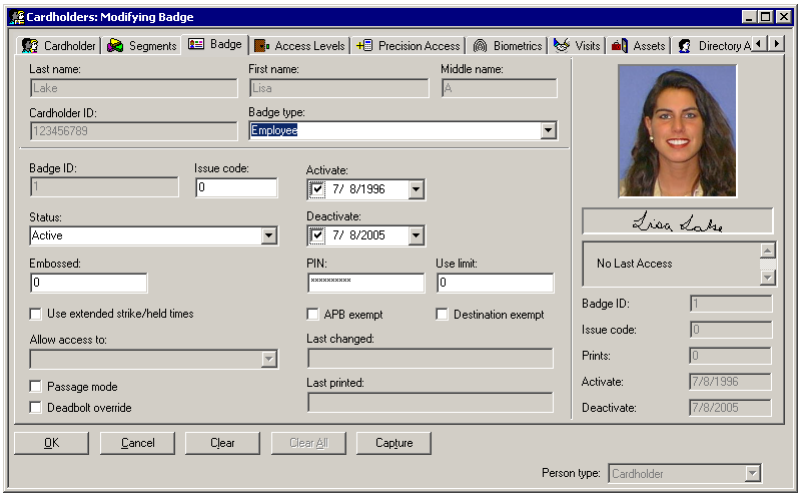
exist for the cardholders in your group to be replaced with the new assignments you select.

4. Click [Next].
5. Select which primary segment you want the selected groups of cardholders to be assigned to.
6. If you selected the **Set the exact assignments** radio button in step 3, and if you want to assign additional segments (if any exist), click on an entry in the **Segments** listing window to select it. You can select multiple entries.
7. Click [Next]. If you selected "All Segments" in step 5, proceed to step 10.
   If you selected the **Make changes to segment assignments** radio button in step 3:
   a. From the **Segments** listing window, select any assignments you want to add in addition to the primary segment.
   b. Click [Next].
   c. If there are segment assignments you want to remove from the group, click on an entry in the **Segments** listing window to select it. You can select multiple entries.
   d. Click [Clear] to remove the assignment.
   e. Click [Next].
8. If you want to perform preliminary validation and be prompted with the results before proceeding, select the **Perform preliminary validation and prompt for confirmation** radio button. Select the **Prompt only if a problem is found** checkbox if you do not want to a prompt for confirmation if there is no validation problem.
   If you do not want to be prompted, select the **Skip preliminary validation and perform the operation without prompting** radio button.
9. Click [Next].
10. Click [Finish].
    - If you selected the **Skip preliminary validation and perform the operation without prompting** radio button in step 8 or if you selected "All Segments" in step 5, the **Bulk Action Results** window opens and displays a summary of your modifications. Click [OK].
    - If you selected the Perform preliminary validation and prompt for confirmation radio button in step 8 and a problem was found, the Bulk Segment Validation Results window opens.
      a. Click [View Badges]. An explanation of the problem is displayed.
      b. Click [OK].
      c. Click [Continue]. The **Bulk Action Results** window opens and displays a summary of your modifications.
      d. Click [OK].

Badge Form (View Mode)



Badge Form (Modify Mode)



Cardholders Folder - Badge Form

Form Element	Type	Comment
Badge listing window	display	Displayed in view mode. Lists all badges for the selected cardholder.
Badge ID	numeric	In add and modify mode, displays the numeric identifier that is assigned to this badge.

Cardholders Folder - Badge Form (Continued)

Form Element	Type	Comment
Issue code	numeric	Displayed in add or modify mode. Indicates the selected badge's issue code if your installation uses issue codes on its badges. **Note:** Issue codes are required for guest badges.
Activate	numeric/drop-down calendar	Displayed in add or modify mode. Indicates the date when the selected badge becomes valid. The current date (at the time the badge record is created) is entered by default, but you can change this value by typing a numeric date into the field, or by selecting a date from the drop-down calendar. • To select a month, click on the and navigation buttons. • You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it. • Navigate to a year by clicking on the displayed year to access the year spin buttons . • Once you have selected a month and a year, click on the day that you want the selected badge to activate on.

Cardholders Folder - Badge Form (Continued)

Form Element	Type	Comment
Deactivate	numeric/drop-down calendar	Displayed in add or modify mode. Indicates the date when the selected badge becomes invalid. A default date is assigned based on the **Badge type**, but you can change this value by typing a numeric date into the field, or by selecting a date from the drop-down calendar. • To select a month, click on the and navigation buttons. • You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it. • Navigate to a year by clicking on the displayed year to access the year spin buttons . • Once you have selected a month and a year, click on the day that you want the selected badge to deactivate on.
Status	drop-down list	Displayed in add or modify mode. Indicates the badge status for the selected badge. Status drop-down list choices are defined on the Simple Lists form of the List Builder folder.
PIN	numeric	Displayed in add or modify mode. Indicates the personal identification number for the selected badge. PIN numbers are used in conjunction with card readers that are operating in “Card and Pin,” or “Pin or Card,” mode. The maximum PIN length is determined by the **PIN type** field in the Access Panels folder. For increased security, PIN codes are not viewable by any user. However, if the system is configured to randomly generate a new PIN code when adding a badge, the user can see the PIN code when they first add the badge (but not later).A user can see the PIN code for guest type badges.
Use limit	numeric	Displayed in add or modify mode. Imposes a restriction on the number of times a cardholder can use his/her badge at readers marked with the “Enforce Use Limit” option.
APB exempt	checkbox	Displayed in add or modify mode. When this checkbox is selected, any anti-passback violation for the selected badge will granted access into the anti-passback area with no violation noted in the Alarm Monitoring application.

Cardholders Folder - Badge Form (Continued)

Form Element	Type	Comment
Destination exempt	checkbox	Displayed in add or modify mode. Select this checkbox if you want the selected badge record to be exempt from destination assurance processing. When selected, the badge will not be included in the destination assurance processing and no alarms will be generated if the cardholder violates any of the destination assurance settings. Via the Reports folder, you can run a Destination Assurance Exempt Cardholders report to see a list of which cardholders will be exempt from processing. For more information refer to the Destination Assurance Folder Chapter in the System Administration User Guide.
Use extended strike/held times	checkbox	Displayed in add or modify mode. When this checkbox is selected, extended held open and extended strike times will be used for the selected badge. **Note:** This option is supported by Best hardware only.
Embossed	numeric	Displayed in add or modify mode. If applicable, enter in this field any numbers or characters that are embossed on the card. Typically this applies to Proximity cards, which are embossed by the manufacturer prior to delivery.
Allow Access To	drop-down list	Displayed only when a valid guest class badge type is selected. Valid guest class badge types are those badge types which were configured during their creation to provide guest parameters. For more information refer to the Badge Types Folder chapter in the System Administration User Guide. Choices in the drop-down list include readers/locks that are associated with the selected badge type. Select an option from the list if you want to assign the selected cardholder to a specific guest reader/lock. The **Badge ID** and **Issue Code** fields are automatically updated when a cardholder is assigned to a guest reader/lock. The values for these fields are obtained from the next available badge ID from the badge numbers reserved for the selected reader, and the next valid issue code for that badge number. The values are updated after you select an item for the drop-down list and then move on to another field on the form. **Note:** This field is subject to licensing restrictions.
Passage Mode	checkbox	Select this checkbox if you want the selected cardholder to have passage mode privileges. The passage mode privilege lets a cardholder use their card twice (within the lock's unlock duration) to place the lock in an unlock mode for an indefinite duration. The door remains unlocked until a card with the passage mode feature is used to relock the door or until a timezone with the “locked” mode becomes effective. **Note:** This field is subject to licensing restrictions.

Cardholders Folder - Badge Form (Continued)

Form Element	Type	Comment
Deadbolt Override	checkbox	If this checkbox is selected, the selected cardholder will have deadbolt override privileges. The deadbolt override privilege lets the cardholder access a door with a deadbolt function mortise lock even when the deadbolt is thrown. **Note:** This field is subject to licensing restrictions.
Last changed	display	Displayed in add or modify mode. Indicates the date when the selected badge record was last saved.
Last printed	display	Displayed in add or modify mode. Indicates the most recent date that the selected badge was printed.

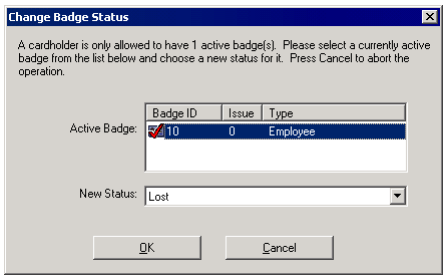
Badge Form Procedures

Add a Badge Record

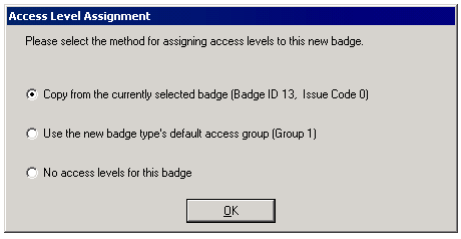
1. Select the **Badge Info** from the **View** menu.The Cardholders folder opens.
2. Select the Badge tab.
3. Locate the cardholder record for which you want to create a badge.
4. Click [Add].
5. Select a **Badge type** from the drop-down list. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.
6. Refer to the Badge form field table and enter the appropriate information into the activated fields in the middle-left section of the Badge form.

Note: Some information is assigned by the system and you may or may not be able to change it.

7. Click [OK] to save the record. If this is the only active badge assigned to this cardholder, you're done and do not need to proceed to the next step.
8. If another active badge was previously assigned to this cardholder, the **Change Badge Status** window will open.



9. The current active badge is displayed in the **Active Badge** display. A cardholder is only allowed to have one active badge. You must change the status of the current active badge to "Lost" or "Returned" in order to assign a new active badge. Select "Lost" or "Returned" from the **New Status** drop-down list.
10. Click [OK]. The **Access Level Assignment** window opens.


Access Level Assignment
Please select the method for assigning access levels to this new badge.
Copy from the currently selected badge (Badge ID 13, Issue Code 0)
Use the new badge type's default access group (Group 1)
No access levels for this badge
OK

11. Do one of the following:
    - If you want the new active badge to have the same access level assignment as the previous active badge, select the **Copy from the currently selected badge** (**Badge ID *n***, **Issue Code *n***) radio button.
    - If you want the new active badge's access assignment level to be the selected badge type's default access group, select the **Use the new badge type's default access group** radio button. If no access groups have been assigned to the selected badge type, this option is not available.
    - Access groups are assigned to badge types in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.
    - If you do not want to assign access levels to the new active badge at this time, select the **No access levels for this badge** radio button.
12. Click [OK].

Modify a Badge Record

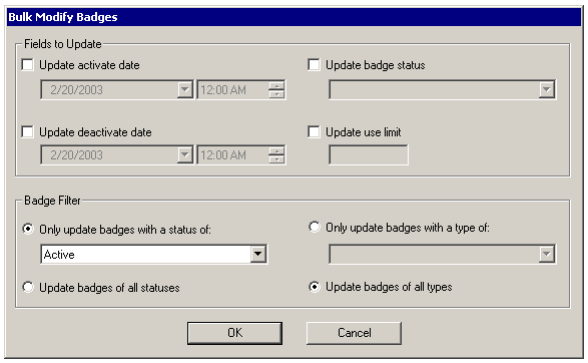
1. Locate the badge record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.

Note: If the PIN type is modified on the Access Panel and/or the General Cardholder Options form, you must log off/log on before you modify a cardholder's pin number.

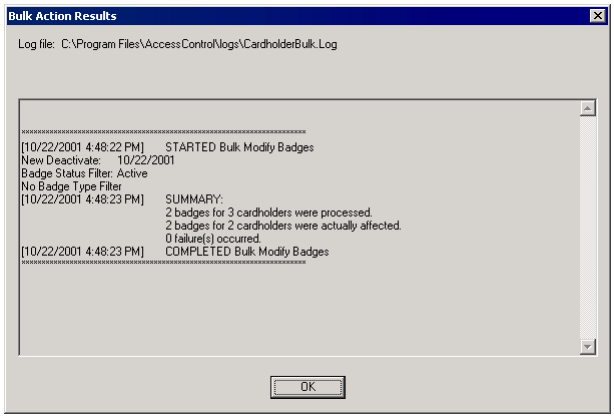
4. Click [OK] to save the changes, or the [Cancel] button to revert to the previously saved values.

Modify Badges for a Selected Group of Cardholders

1. Locate the group of cardholders whose records you want to modify.
2. Select **Bulk** > **Modify Badges** from the **Cardholder** menu. The **Bulk Modify Badges** window opens.



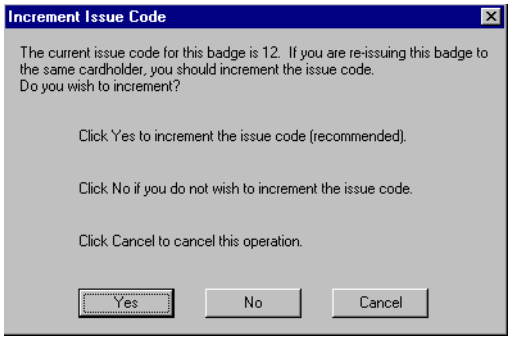
3. If you want to update fields, chose which fields you want to update. You can:
   - Select the **Update Activate Date** checkbox and enter a new activate date and/or time to be assigned to the selected group of badges.
   - Select the **Update Deactivate Date** checkbox and enter a new deactivate date and/or time to be assigned to the selected group of badges.
   - Select the **Update Badge Status** checkbox and enter a new status to be assigned to the selected group of badges.
   - Select the **Update Use Limit** checkbox and enter a new use limit to be assigned to the selected group of badges.
4. If you want to filter which badges from the selected group will get modified, do so in the **Badge Filter** section. You can filter by badge status and/or badge type.
   If you do not want to filter badges, check the **Update badges of all Statuses** and **Update badges of all Types** radio buttons.
5. Click [OK]. A message will be displayed asking if you want to continue with the modification.
6. Click [Yes]. The **Bulk Action Results** window opens and displays a summary of your modifications.

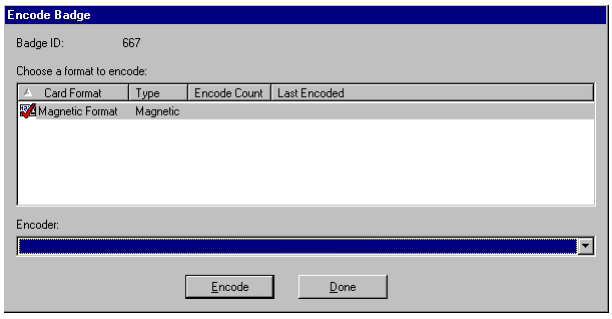

Bulk Action Results
Log file: C:\Program Files\AccessControl\logs\CardholderBulk.Log
[10/22/2001 4:48:22 PM] STARTED Bulk Modify Badges
New Deactivate: 10/22/2001
Badge Status Filter: Active
No Badge Type Filter.
[10/22/2001 4:48:23 PM] SUMMARY:
2 badges for 3 cardholders were processed.
2 badges for 2 cardholders were actually affected.
0 failure(s) occurred.
[10/22/2001 4:48:23 PM] COMPLETED Bulk Modify Badges
OK

7. Click [OK].

Encode Badge Configurations

1. Locate the badge record that you want to encode onto a smart card.
2. Click [Encode]. If the selected badge record has a “guest” badge type, the Increment Issue Code window opens. If the selected badge record has a badge type other than “guest,” the Encode Badge window opens.


Increment Issue Code
The current issue code for this badge is 12. If you are re-issuing this badge to the same cardholder, you should increment the issue code.
Do you wish to increment?
Click Yes to increment the issue code (recommended).
Click No if you do not wish to increment the issue code.
Click Cancel to cancel this operation.
Yes
No
Cancel



3. If the Encode Badge window is open, select a format to encode and an **Encoder**, then click [Encode].
4. If the Increment Issue Code window is open, click [Yes].

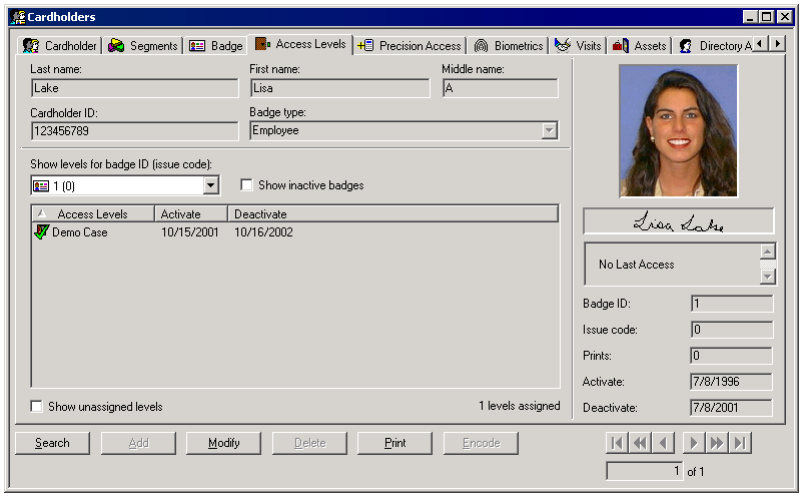
Notes: If you get a transport key verification error when you attempt to encode a Biocentric smart card, be sure to verify a valid transport key is listed in the Registry Editor.

To do this, click Start > Run, enter “regedit” and click [OK]. Navigate to My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Biocentric Solutions\Enrollment\Settings. Right-click **SCTransportkey** and select modify. Update the transport key setting to match the transport key programmed into the smart card.

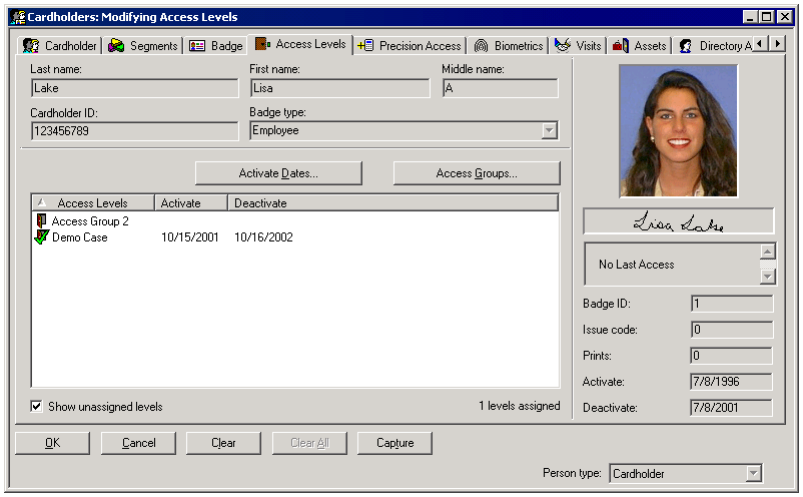
Delete a Badge Record

1. Locate the badge record you want to delete.
2. Click [Delete].
3. Click [OK].

Access Levels Form (View Mode)



Access Levels Form (Modify Mode)



Cardholders Folder - Access Levels Form

Form Element	Type	Comment
Show levels for badge ID (issue code)	drop-down list	Displayed in view mode. Lists the badge ID and issue code (in parentheses) for the current active badge. If the **Show inactive badges** checkbox is selected, the list includes both the active and the inactive badge(s) assigned to the selected cardholder. Select a badge ID (issue code) from the list and the corresponding access levels for that badge will be displayed in the **Access levels** display.

Cardholders Folder - Access Levels Form (Continued)

Form Element	Type	Comment
Show inactive badges	checkbox	Displayed in view mode. When selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.
Access levels display	display	Displayed in a view and modify mode. When the **Show unassigned levels** checkbox is selected, lists both access levels that **have been** and that **can be** assigned to the selected cardholder/badge record. If the **Show unassigned levels** checkbox is not selected, only access levels that **have been** assigned will be listed. If they exist, also displays the access level's activation and deactivation dates.
Show unassigned levels	checkbox	Displayed in view and modify mode. When selected, the **Access levels** display lists both access levels that **have been** and that **can be** assigned to the selected cardholder/badge record.
Number of levels assigned	display	Displayed in view and modify mode. Displays the number of access levels that have been assigned to the selected cardholder/badge record. For example: 6 levels assigned.
Activate Dates	push button	Displayed in modify mode. When selected, displays the Access Level Activation Dates form from where you can select the dates when the selected access level will become valid and invalid.
Access Groups	push button	Displayed in modify mode. When selected, displays the Select Access Levels in a Group form from where you can choose the access level group that you want to select access levels from.

Access Levels Form Procedures

Assign Access Levels to a Badge

1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Access Levels tab.
3. Locate the cardholder record for which you want to assign access levels.
4. From the **Show levels for badge ID (issue code)** drop-down list, select the badge you want to assign access levels to.

Note: If the **Show inactive badges** checkbox is selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.

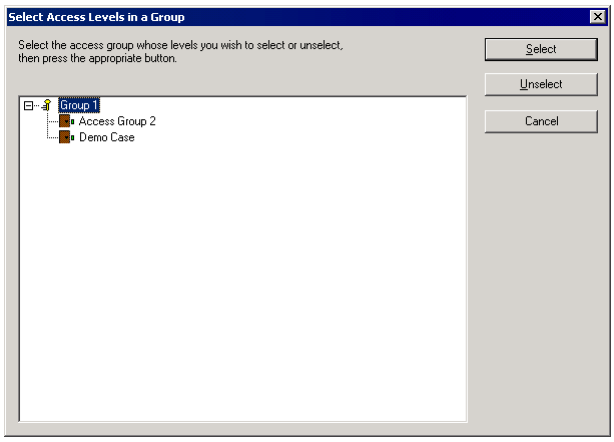
---

5. Click [Modify].
6. Select the **Show unassigned levels** checkbox. The **Access levels** display will list both access levels that **have been** and that **can be** assigned to the selected cardholder/badge record.

Note: To find out more about a particular access level, either double-click on an access level entry, or right-click on an access level entry and select **Level Definition**. A popup window opens, listing the reader/time zone combinations that define the access level. For example:

Access Level 4
Bldg. 23-1 Rdr 1 Master + Hourly Employees
Bldg. 23-1 Rdr 1 Slave + Salaried Employees
Bldg. 23-2 Rdr 1 Master + Hourly Employees
Bldg. 23-2 Rdr 1 Slave + Salaried Employees
Bldg. 7 DL Rdr 1 + All Floors Always

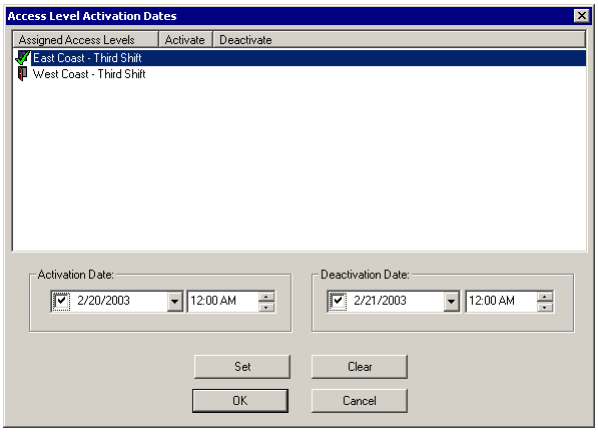
7. Click on an access level in the **Access levels** display to select it.
   Optional: If you want to assign all the access levels that belong to an access group:
   a. Click [Access Groups]. The **Select Access Levels in a Group** window opens.


Select Access Levels in a Group
Select the access group whose levels you wish to select or unselect, then press the appropriate button.
Select
Unselect
Cancel
Group 1
Access Group 2
Demo Case

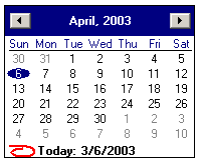
   b. The **Select Access Levels in a Group** window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.
   c. Click [Select].
   d. Click [Yes].
8. Repeat step 7 for each access level you want to assign.
9. Click [OK].

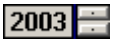
Assign Activation and Deactivation Dates to Access Levels

1. On the Access Levels form, click [Modify].
2. The access levels listing window displays all access levels that are currently configured for use with the selected cardholder's badge type. From the listing window, select one or more access levels.
3. Click [Activate Dates]. The Access Level Activation Dates window opens. The selected access levels that have been assigned to the selected cardholder/badge record will be listed in the Assigned Access Levels listing window.



4. Click on an access level entry to select it.
5. In the Activation Date section:
   a. Type a numeric date into the field, or select a date from the drop-down calendar.



   - To select a month, click on the and navigation buttons.
   - You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
   - Navigate to a year by clicking on the displayed year to access the year spin buttons  .
   - Once you have selected a month and a year, click on the day that you want the selected badge to activate on.

   b. If your system is configured so that you can specify a specific activation time, enter a time in the field to the right of the date field. This time will be used in conjunction with the selected activation date.

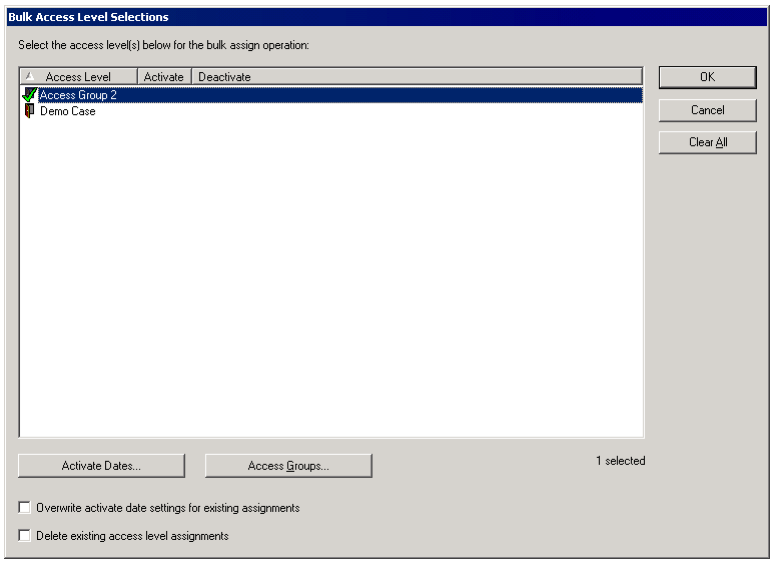
Notes: To specify the activation time, the **Store expiration date** field on the Options sub-tab of the Access Panels form must be set to **Date only** or **Date and time**. The Date and time option applies to Best panels only, while the Date only option applies to Best and Apollo panels but not Offline Lock panels.

The activation time you enter should match the granularity setting on the Cardholder Options folder, General Cardholder Options form. Otherwise, the time you enter will be rounded down. For example if the granularity is set to 30 minutes, and you enter any time between 4:00 and 4:29 the time will automatically be rounded to 4:00. Any time entered between 4:31 and 4:59 will be rounded to 4:30.

6. In the Deactivation Date section, repeat step 5, choosing the date when you want the selected badge to become invalid.
7. Click [Set].
8. Repeat steps 4-7 for each access level entry.
9. Click [OK].

Assign Access Levels to a Selected Group of Cardholders

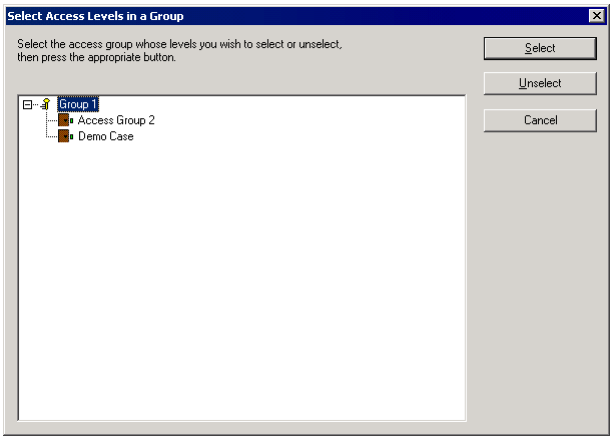
1. Locate the group of cardholders that you want to assign access levels.
2. Select **Bulk** > **Assign Access Levels** from the **Cardholder** menu. The **Bulk Access Levels Selections** window opens.



3. Click on the access level you want to assign to select it. You can select multiple entries.
   Optional: If you want to assign all the access levels that belong to an access group:
   a. Click [Access Groups]. The **Select Access Levels in a Group** window opens.

      The **Select Access Levels in a Group** window lists all currently defined access groups. You can expand an entry to display the list of access

levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.


Select Access Levels in a Group
Select the access group whose levels you wish to select or unselect, then press the appropriate button.
Select
Unselect
Cancel
Group 1
Access Group 2
Demo Case

b. Click [Select].

c. Click [Yes].

4. If you want to define the activation and deactivation dates, click [Activate Dates]. For more information, refer to Assign Activation and Deactivation Dates to Access Levels on page 166.

5. Select the **Overwrite activate date settings for existing assignments** if you modified the activation and/or deactivation dates and you want your changes to overwrite existing assignments.

6. Select the **Delete existing assignments** checkbox if you want to delete all existing access level assignments for the selected cardholder/badge records and replace them with your bulk selections.

7. Click [OK].

Note: **All** active badges will be affected by this change, even in multiple active badge environments.

Remove Access Levels From a Selected Group of Cardholders

1. Locate the group of cardholders that you want to remove access levels from.
2. Select **Bulk** > **Remove Access Levels** from the **Cardholder** menu. The **Bulk Access Levels Selections** window opens.
3. Click on the access level you want to remove to select it. You can select multiple entries.
   Optional: If you want to remove all the access levels that belong to an access group:
   a. Click [Access Groups]. The **Select Access Levels in a Group** window opens.
   b. The **Select Access Levels in a Group** window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.
   c. Click [Select].
   d. Click [Yes].
4. Click [OK].

Note: **All** active badges will be affected by this change, even in multiple active badge environments.

Modify Access Levels Assignments

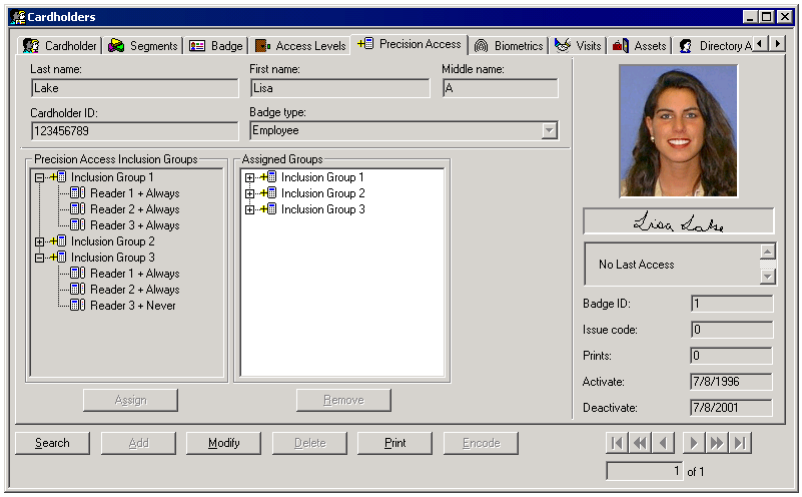
1. Locate the cardholder/badge record whose access level assignments you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete Access Levels Assignments

1. Locate the cardholder/badge record whose access level assignments you want to delete.
2. Click [Delete].
3. Click [OK].

Precision Access Form

Note: The Precision Access tab is only displayed if either "Inclusion" or "Exclusion" is selected in the **Precision Access Mode** field on the General Cardholder Options form of the Cardholder Options folder in the System Administration software application.



Cardholders Folder - Precision Access Form

Form Element	Type	Comment
Precision Access Inclusion/ Exclusion Groups	display	Lists all currently defined Exclusion or Inclusion groups (your system will have one or the other) and the readers and timezones/elevator control levels that belong to each. A icon precedes each exclusion group entry. An icon precedes each inclusion group entry. Exclusion or Inclusion groups are defined on the Precision Access form of the Access Levels folder.
Assigned Groups	display	Lists the Inclusion/Exclusion Groups assigned to the selected cardholder/badge record.
Assign	push button	Assigns to the selected cardholder/badge record the access levels selected in the Precision Access Inclusion/Exclusion Groups field.
Remove	push button	Removes from the current cardholder/badge record the access levels selected in the Precision Access Inclusion/Exclusion Groups field.

Precision Access Form Procedures

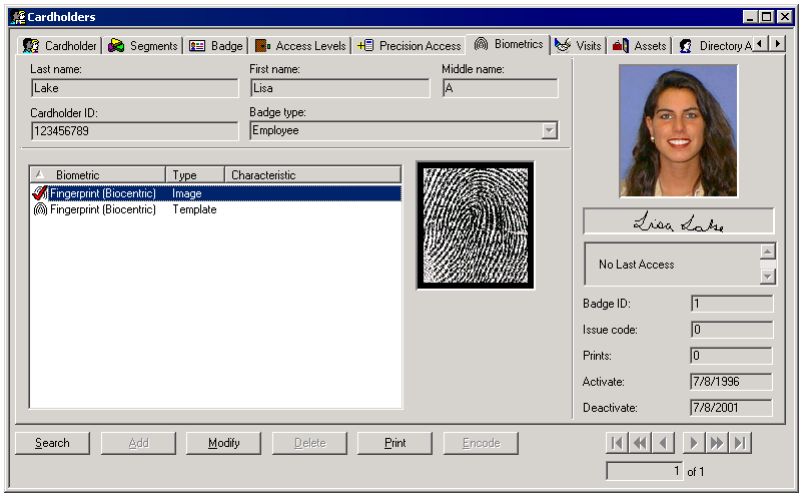
Assign Precision Access Groups to a Badge

1. Select the **Badge Info** from the **View** menu.The Cardholders folder opens.
2. Select the Precision Access tab.
3. Locate the cardholder record that you want to assign precision access. Precision access can only be assigned to the selected cardholder's/visitor's active badge.
4. Click [Modify].
5. In the **Precision Access** [**Inclusion** or **Exclusion**] **Groups** window, select a precision access group.
   - The window contains all currently defined precision access groups. You can expand an entry to display the list of readers (if entries are Exclusion groups) or readers and timezones (if entries are Inclusion groups) that make up the group.
   - You can select only one group at a time.
   - By selecting a precision access group you select all of the reader-timezone combinations it contains. These combinations are defined on the Precision Access form of the Access Levels folder.
6. Click [Assign]. The group(s) you selected will be listed in the **Assigned Groups** window.
7. Repeat steps 5 and 6 for each additional group you want to assign to the badge. You can assign multiple Exclusion or Inclusion groups in addition to the 6 access levels that a cardholder can normally have.
8. Click [OK].

Remove Precision Access Groups From a Badge

1. Locate the record of the cardholder whose precision access assignment you want to remove.
2. In the **Assigned Groups** window, select the precision access group to be removed.
3. Click [Remove].
4. Repeat steps 2 and 3 for each precision access group you want to remove.
5. Click [OK].

Biometrics Form



Cardholders Folder - Biometrics Form

Form Element	Type	Comment
Biometric listing window	display	In search mode, lists all biometric features and the type associated with each.
		In view mode, lists the selected cardholder's biometric information (if any exists).
		There are three biometric features, **Fingerprint**, **Hand Geometry** and **Iris**. A biometric fingerprint's type can be **Template** or **Image**.
		Fingerprint • A template of the cardholder's fingerprint is encoded on the ID card. For more information refer to the Multimedia Capture Module appendix in the System Administration User Guide. When an ID card is presented to a reader, it will compare the stored template with the cardholder's actual fingerprint for verification. • A fingerprint image is a visual representation of the cardholder's fingerprint that is independent from the template. For more information refer to the Multimedia Capture Module appendix in the System Administration User Guide.

Cardholders Folder - Biometrics Form (Continued)

Form Element	Type	Comment
Biometric listing window	display	**Hand Geometry** • A hand geometry template is a representation of the cardholder's handprint that is stored in the database. For more information refer to the Multimedia Capture Module appendix in the System Administration User Guide. • When an ID card is presented to the primary access control reader (a hand geometry reader is considered an alternate reader that is used in association with a primary reader, such as a magnetic stripe or proximity reader) it will ask for verification from the alternate reader. The system will compare the stored hand geometry template with the cardholder's actual handprint for verification. • A primary access control reader will only ask for verification from the hand geometry reader when the **Verify Mode** checkbox (located on the Settings form in the Readers folder) is selected. For more information refer to the Readers folder in the System Administration User Guide.
Fingerprint image	display	Displayed in view mode. Displays a visual representation of the cardholder's fingerprint. For more information refer to the Multimedia Capture Module appendix in the System Administration User Guide.
Search Type	drop-down list	Displayed in search mode. This field is used in conjunction with the listing window. Click on a biometric feature in the listing window and select a choice from the **Search Type** drop-down list to search for a record that **Has** or **Does Not Have** a fingerprint image, a fingerprint template, iris data, or a hand geometry template associated with the cardholder.

Biometrics Form Procedures

Search for a Cardholder's Biometric Record

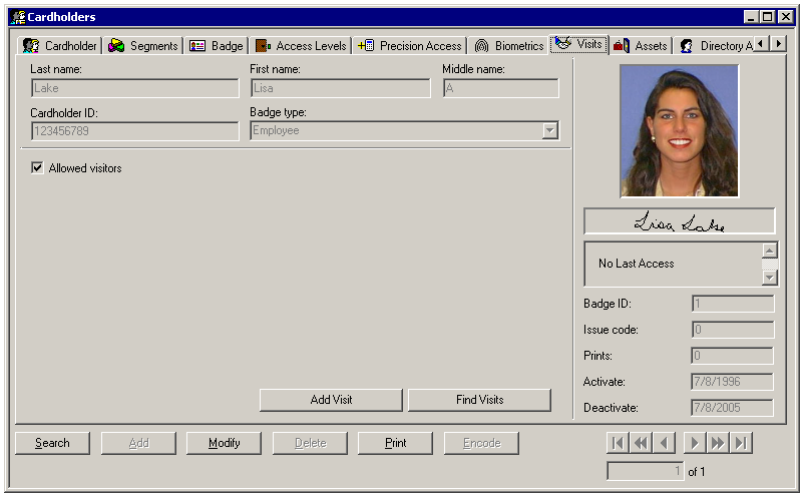
1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Biometrics tab.
3. Click [Search].
4. In the **Biometric** listing window, click on a biometric feature to select it.
5. Choose either "Has" or "Does Not Have" from the **Search Type** drop-down list to search for a record that has or does not have a fingerprint image, a

fingerprint template, iris data, or a hand geometry template associated with the cardholder.

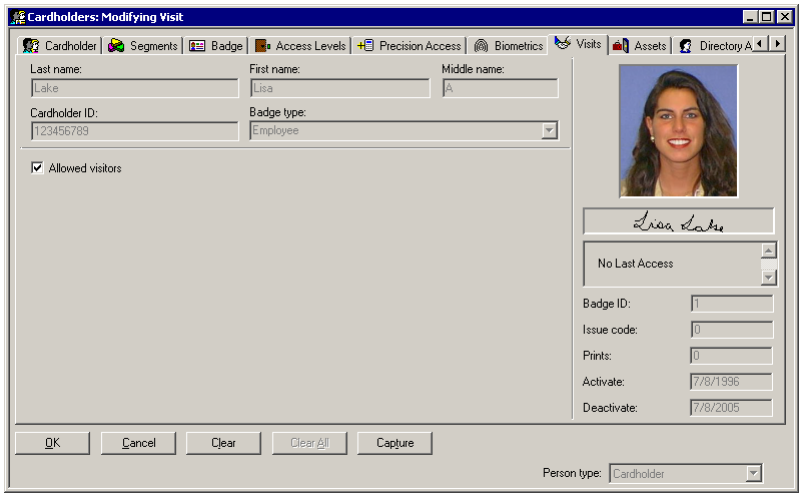
6. Click [OK].

   B.A.S.I.S. retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Visits Form (View Mode)



Visits Form (Modify Mode)



Cardholders Folder - Visits Form

Form Element	Type	Comment
Allowed visitors	checkbox	When selected in modify mode, the selected cardholder is allowed to be assigned visitors. When not selected, the cardholder will not be available for visit assignment in the Visitor Management application.

Cardholders Folder - Visits Form (Continued)

Form Element	Type	Comment
Add Visit	push button	In modify mode, click this button to display the Adding Visit window. From here you can add or modify visits, display visit records for a selected date range, and search for visit records based on the scheduled time in, scheduled time out, time in, time out, or date and time last changed.
Find Visits	push button	This button quickly looks up visit records associated with the record whose name is specified in the **Last name**, **First name** and **Middle name** fields.
Type	drop-down list	Displayed in modify mode. Indicates the type of visit.
Purpose	text	Displayed in modify mode. Indicates the purpose of the visit.

Visits Form Procedures

Modify a Cardholder's Permission to Have Visitors

A cardholder must have permission to be allowed to have visitors visit. This permission can only be granted (or taken away) in System Administration or ID CredentialCenter, but not in Visitor Management. To change a cardholder's permission to have visitors:

1. Select the **Badge Info** from the **View** menu.
2. Click the Cardholders tab.
3. Locate the record of the cardholder that you want to allow visitors.

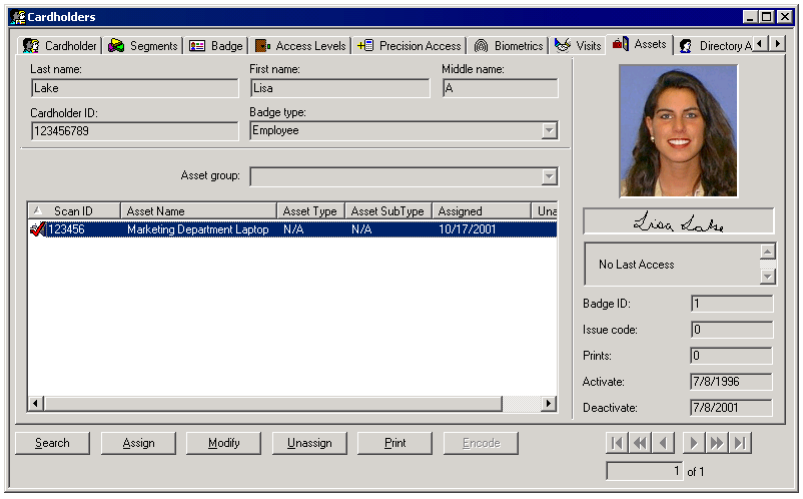
Note: Cardholders who are visitors cannot be assigned visitors.

4. Click the Visits tab.
5. Click [Modify].
6. The **Allowed visitors** checkbox setting controls a cardholder's permission to have visitors. Select the setting you want for the selected cardholder. The two possible settings are:
   - When the **Allow visitors** checkbox is selected, the cardholder will be allowed to have visitors. Only cardholders with the Allow visitors checkbox will be returned when searching for a cardholder and attempting to add a new visit.
   - When the **Allow visitors** checkbox is not selected, no visits to the cardholder can be scheduled.

Note: Changing the **Allow visitors** checkbox setting for a cardholder will only change the cardholder's ability to have visitors after the setting has been changed; any previously scheduled visits will be allowed to occur.

7. Click [OK].

Assets Form



Cardholders Folder - Assets Form

Form Element	Type	Comment
Asset group	drop-down list	Indicates the asset group to which the cardholder or visitor belongs.
Asset listing window	display	Lists all assets that are currently assigned to the selected cardholder or visitor.
Assign	push button	When selected, assigns an asset to a cardholder.
Unassign	push button	When selected, unassigns an asset.

Assets Form Procedures

Assign an Asset to a Cardholder

1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Assets tab.
3. Locate the cardholder record for which you want to assign the asset.
4. On the Assets form of the Cardholders folder, locate the asset record that you want to assign.
5. Click [Assign].

Note: Authorized users can manually assign an asset to a cardholder who does not have proper asset group permissions for that asset.

Unassign an Asset

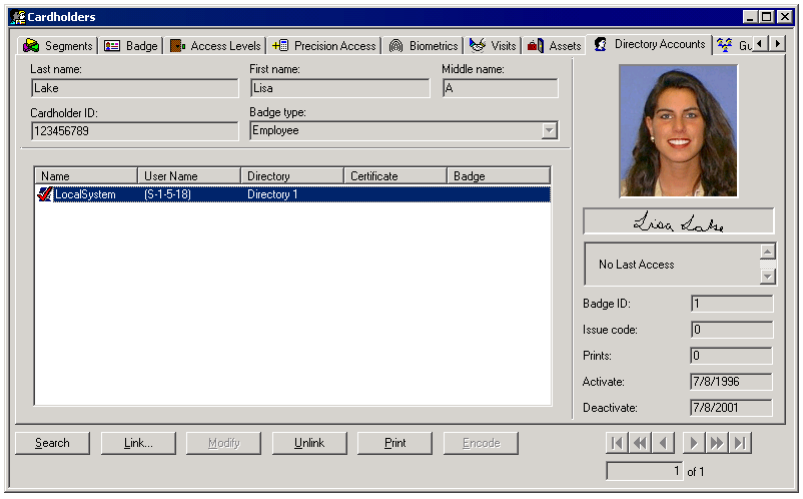
1. In the **Asset** listing window, click on the name of an asset to select it.
2. Click [Unassign].

Modify the Asset Group

1. Locate the cardholder record for which you want to modify.
2. Click [Modify].
3. Select an Asset Group from the drop-down list.
4. Click [OK].

Note: A record can only be modified if an asset group was assigned when the cardholder or visitor was added.

Directory Accounts Form



Cardholders Folder - Directory Accounts Form

Form Element	Type	Comment
Directory accounts listing window	display	Lists the directory accounts that have been linked to the selected cardholder.
Link	push button	When selected, displays the **Select Account** window from where you can link a directory account to the selected cardholder.
Unlink	push button	When selected, unlinks the selected cardholder from the directory account that is selected in the Directory Accounts listing window.

Directory Accounts Form Procedures

Link a Cardholder to a Directory Account

1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Directory Accounts tab.
3. Locate the cardholder record for which you want to link a directory account.
4. Click [Link]. The Select Account window opens. In the Select Account window:
   a. In the **Directory** drop-down list, select the directory you wish to link to.
   b. In the **Field** drop-down list select whether to search for a name or user name.
   c. In the **Condition** drop-down list, select how the value will be related to the field. For example, a search where the **Field** selected is “Name”, the **Condition** selected is “contains” and the **Value** specified is “Lake” will

display all accounts where the name contains the word “Lake”, such as Lisa Lake.

d. In the **Value** field, type or select a word you think may be in the user name or name. If you leave this field empty, all accounts for the selected directory will be displayed when the search is executed.

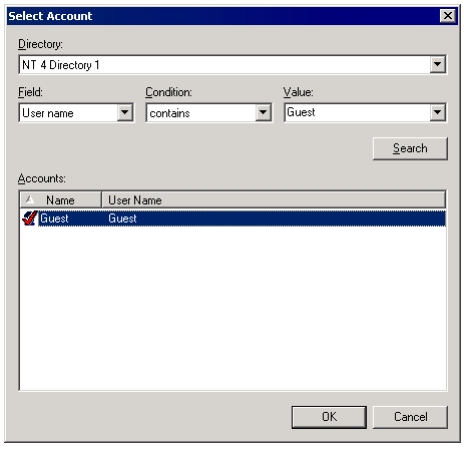
Note: To help you search, the **Value** field will contain different ways that the selected account may be expressed. For example, if the user account Lisa Lake is selected, the permutations listed might be “L. Lake”, “LISA”, “Lisa”, “Lisa L.”, “Lisa Lake”, “LL”, “Lake” and “Lake, Lisa.”

---

e. Click [Search].

f. The accounts associated with the selected **Directory** will be displayed in the Accounts listing window.

- If the account you wish to link to is displayed, select it. Your window should look similar to the following:



- If the account you wish to link to is not displayed, return to step d and select another **Value** to search for.

g. Click [OK].

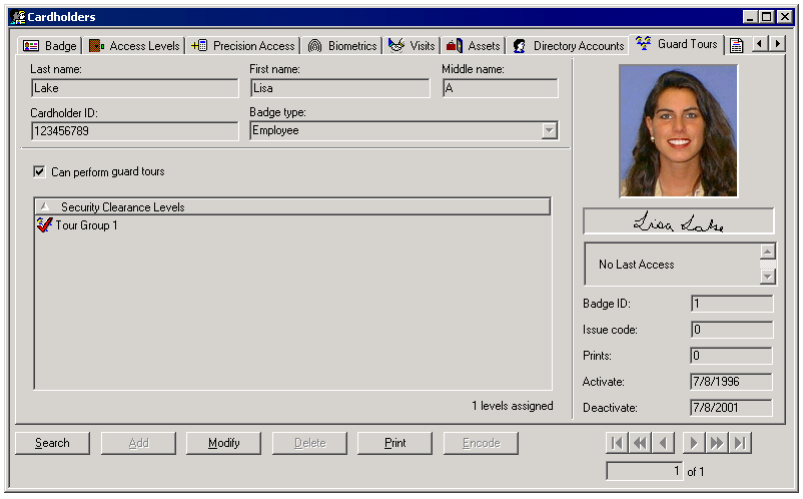
h. Repeat steps 3 and 4 for each directory account you wish to link to the selected user account.

5. Click the [OK] button on the Directory Accounts form.

Unlink a Directory Account

1. Locate the record of the cardholder you want to unlink a directory account from.
2. Click on an entry in the **Directory accounts** listing window to select it.
3. Click [Unlink].
4. Click [OK].

Guard Tours Form



Cardholders Folder - Guard Tours Form

Form Element	Type	Comment
Can perform guard tours	checkbox	Select this checkbox to if you want the selected cardholder to perform guard tours.
Security Clearance Levels listing window	display	Lists all security clearance levels that have been configured in the system. Security clearance levels are a means of limiting the number of tour guards to choose from when a tour is launched. Particular security clearance levels will be assigned only to guards who will need access to areas where a tour will take them. When a tour is launched, only guards with the appropriate security clearance level for that tour will be listed. Guard tours and security clearance levels are configured in the Guard Tour folder. For more information refer to the Guard Tour Folder chapter in the System Administration User Guide. **Note:** This field is enabled only if the **Can perform guard tours** checkbox is selected.
Number of levels assigned	display	Displays the number of security clearance levels that have been assigned to the selected cardholder. For example: 6 levels assigned.

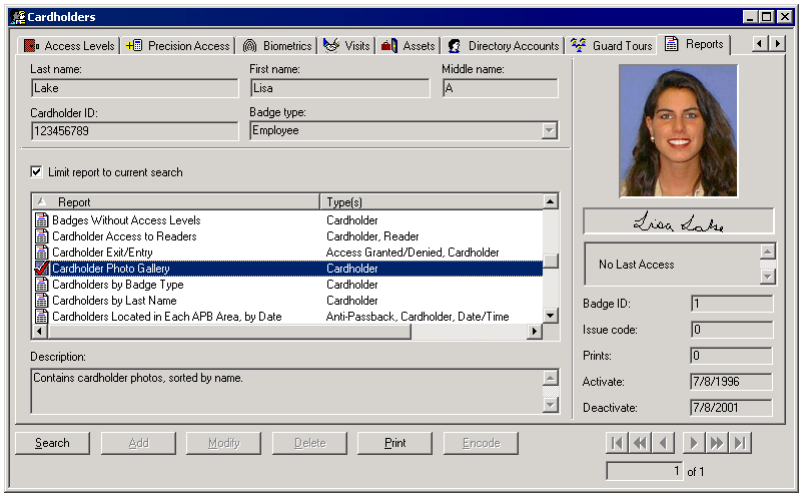
Guard Tours Form Procedures

Assign Guard Tour Security Clearance Levels to a Cardholder

1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Guard Tours tab.
3. Locate the cardholder record for which you want to assign security clearance levels.
4. Click [Modify].
5. Select the **Can perform guard tours** checkbox.
6. In the **Security Clearance Levels** listing window, click on an entry to select it.
7. Click [OK].

Note: You can assign multiple security clearance levels to a cardholder.

Reports Form



Cardholders Folder - Reports Form

Form Element	Type	Comment
Limit report to current search	checkbox	When selected, only cardholders in the current search will be included in the report.
Report listing window	display	Lists currently defined cardholder-related reports.
Description	display	A brief description of the report contents.

Reports Form Procedures

Run a Cardholder Report

1. Select the **Badge Info** from the **View** menu. The Cardholders folder opens.
2. Select the Reports tab.
3. Locate the cardholder record(s) for which you want to run a report. (If you want to run a report on all cardholder records, skip this step.)
4. In the **Reports** listing window, click on the name of the report you want to run.
5. Select the **Limit report to current search** checkbox if you want only cardholders in the current search to be included in the report. If you do not select this checkbox, all cardholder who meet the criteria specified in the **Description** field will be included in the report.
6. Click [Print]. The **Print Report Options** window opens. For more information, refer to Chapter 17: Print Report Options Window on page 297.

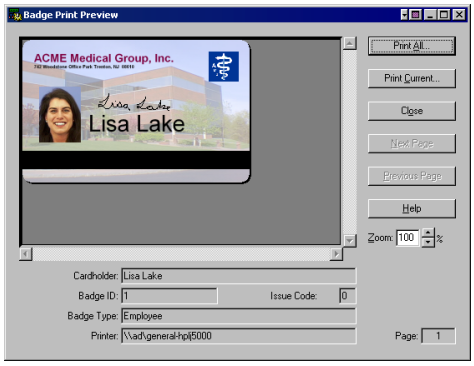
Note: Any report in the **Reports List** Window on the Event Reports form in the Reports folder that has “Cardholder” listed in the **Type(s)** column is available on the Reports form in the Cardholders folder. This means that a report can be generated on the Reports form in the Cardholders folder based on a cardholder search operation.

Chapter 13: Badge Print Preview Window

The Badge Print Preview window is used to:

- View (on-screen) a badge to be printed from the Cardholders folder.
- Print a badge.

This window is displayed by clicking [Print] in the Cardholders folder and then clicking [Print Preview], or by selecting **Print** from the **Application** menu. The **Application** menu is only available in System Administration and ID CredentialCenter.



Badge Print Preview Window

Element	Type	Comment
Preview window	display	Displays the currently selected badge layout with cardholder information.
Print All	push button	Prints all the badges selected according to the Badge Printing window.
Print Current	push button	Prints the badge that is currently displayed in the preview window.
Close	push button	Click on this button to exit from the Badge Print Preview window.
Next Page	push button	Allows you to view the next badge if multiple badges are being printed or to view the back layout of a two-sided badge.
Previous Page	push button	Allows you to view the previous badge if multiple badges are being printed or to view the front layout of a two-sided badge.
Help	push button	Displays online help for this topic.
Zoom	spin buttons	Enter a value to zoom in or zoom out on the badge in the preview window. • Entering a number greater than 100% will cause the preview to zoom in on the badge, displaying less area and more detail • Entering a number less than 100% will cause the preview to zoom out on the badge, display more area and less detail

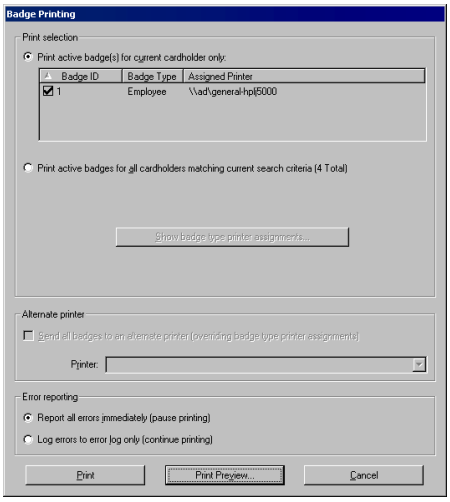
Badge Print Preview Window (Continued)

Element	Type	Comment
Badge information	display	Displays badge and cardholder information for the badge currently in the print preview window. Printer information displays also.
Page number	display	Displays the number of the page or badge that is currently in the preview window.

Badge Print Preview Window Procedures

Preview and Print a Badge

1. Select the badge(s) from within the Cardholders folder (Cardholders, Badge, Access Levels, Assets or Precision Access form).
   - Before printing, make sure that you are properly configured to print badges. Configurations are done using the Badge Types and Card Formats folders in System Administration or ID Credential Center.
   - Make sure the proper printer is chosen. This is configured by selecting **Badge Types** from the **Administration** menu in System Administration or ID Credential Center and setting the printer assignments on the Printing/Encoding folder.
2. Do one of the following:
   - Select **Print** from the **Application** menu.
   - Click [Print] on any form within the Cardholders folder (Cardholders, Badge, Access Levels, Assets or Precision Access form).
3. The Badge Printing window displays.



   - The **Print selection** section determines which badges are printed or previewed out of the cardholders listed in the current search results.

Notes: Badge(s) will NOT print if at least one badge does not have a printer assigned to it or at least one badge has been assigned to a printer that B.A.S.I.S. no longer recognizes.

You must establish a network connection to a remote printer (via control panel) in order B.A.S.I.S. to recognize that printer.

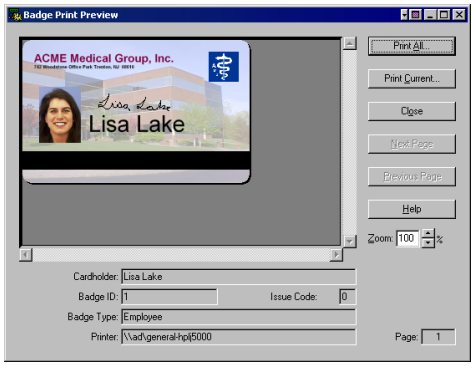
  - To print/preview specific badges for the current cardholder click the **Print active badge(s) for current cardholder only** radio button and select which active badges (if there are multiple active badges) are to be printed or previewed. Only the active badges for the current cardholder display in the **Print selection** section.
  - To print all the active badges for the current cardholder click the **Print active badges for all cardholders matching current search criteria** radio button. If you click [Show badge type printer assignments] the following information displays within the Badge Printing window: Badge Type, Primary Segment and Assigned Printer. Notice the Badge Printing window changes when the [Show badge type printer assignments] button is selected.

- The **Alternate printer** section allows you to override badge type printer assignments and send all badges to an alternate printer. This section is only active when an alternate printer is configured and the user has permission to choose an alternate printer.
- The **Error Reporting** section allows you to configure how printing errors are handled. All badge printing is logged to the transaction log (print previews are not logged).
  - Click the **Report all errors immediately (pause printing)** radio button if you want to be prompted to either abort printing or skip to the next badge (or badge type) when an error occurs.
  - Click the **Log errors to error log only (continue printing)** radio button if you want errors logged and badge printing to continue on to the next badge (or if the error is associated with the badge type, the printing will move onto the next badge type).

4. It is recommended that you preview your badges first before printing them. If there is no need to preview the badge(s), you may print at this time by

clicking [Print]. Skip to step 9. If you wish to exit the window without printing, click [Cancel]. Otherwise continue on to the next step.

5. Click [Print Preview] to display the Badge Print Preview window.



The current badge displays along with cardholder data and printer information.

6. Use the [Next Page] and [Previous Page] buttons to view the next badge or other side of a two-sided badge.

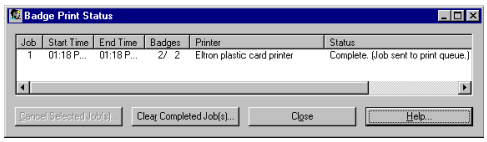
7. You can zoom in or out on the badge by changing the percentage value in the **Zoom** box. A larger number displays the badge close-up, in more detail. A smaller number will display more of the badge, in less detail.

8. To print the badge(s), do one of the following:
   - Click [Print Current]. Doing so will print the badge that is currently in the preview window.
   - Click [Print All] to print all of the badges that have been selected.
   - To exit from the window without printing, click [Close].

Note: If a user attempts to print a badge that has already been printed the maximum number of times then an error displays and the badge does not print. As with other printing errors the user can continue on to the next badge if a batch print is being performed.

---

9. If you decided to print badges a status window displays to indicate the status of the print operation.



A *single* print job entry represents all the badges selected in the **Print selection** section.

Chapter 14: Visits Folder

The Visits folder contains the Status search form, the Visit form, the Details form, the E-mail form and the Reports form with which you can:

- Display visit records for a selected date range
- Search for visit records based on the scheduled time in, scheduled time out, time in, time out or date and time it was last changed
- Display visit records that are scheduled in the future, scheduled and are late, active, active and overstayed and finished
- Filter and display visit records for a selected cardholder, visitor or both
- Display the cardholder or visitor record associated with a visit
- Refresh the Visits listing window
- Send e-mail notifications regarding visits
- Add or modify visits
- Delete a visit or multiple visits
- Print a disposable badge or multiple disposable badges
- Sign out and sign in a visit or multiple visits
- Generate a report for either a defined search criteria or for all visits

Toolbar Shortcut

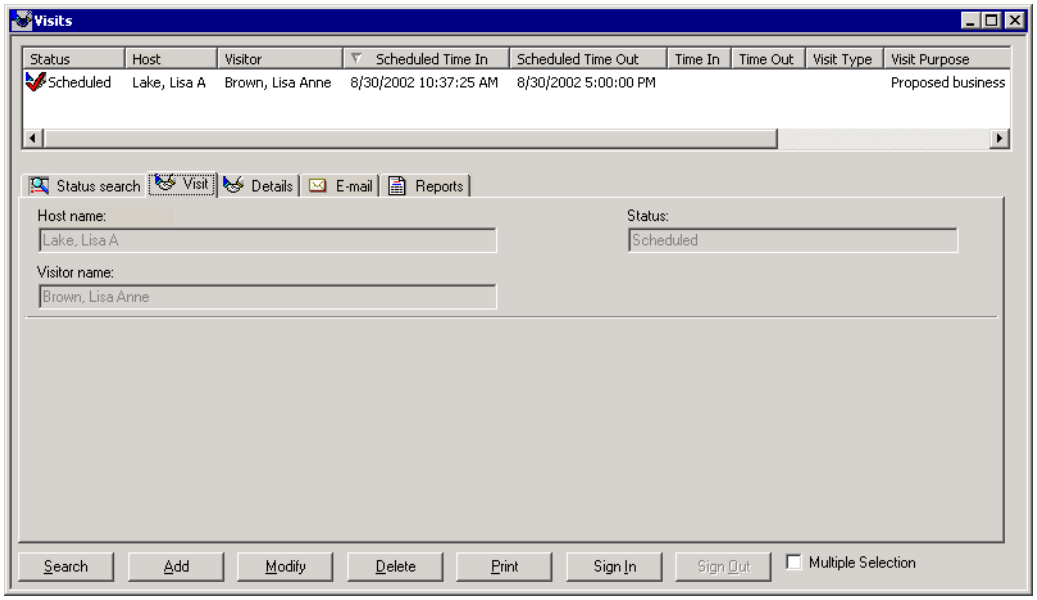
This folder is displayed by selecting **Visits** from the **View** menu.

Visits Folder Overview

The forms in the Visits folder are divided into two sections: the form elements that are common to every form in the Visits folder (shown in the screen shot that follows) and the form elements that are unique to each form. For descriptions of the common form elements refer to Visits Folder Field Table on page 194. For descriptions of the unique form elements refer to:

- Status Search Form Field Table on page 215
- Visit Form Field Table on page 212
- Details Form Field Table on page 217
- E-mail Form Field Table on page 218

- Reports Form Field Table on page 221.



Notes: This documentation refers to visit data fields that are shipped as the default by Best. If you have used the FormsDesigner application to customize your visit data, the elements on your Visits folder forms will be different.

Forms and fields that pertain to segmentation are only available if segmentation is enabled on your system.

Visit Right-Click Menu

If you right-click on a visit in the listing window, a menu will be displayed. The menu contains the following options:

Right-click menu option	Description
Select All	Enabled only when the **Multiple Selection** checkbox is selected. If selected, all visits in the listing window will be selected.
Clear All	If selected, all visits selected in the listing window will be deselected.
Add	Selecting this option does the same thing as clicking the [Add] button - it allows you to add another visit based on the currently selected visit.
Modify	Selecting this option does the same thing as clicking the [Modify] button - it allows you to change the visit that is currently selected.
Delete	Selecting this option does the same thing as clicking the [Delete] button - it allows you to delete the visit that is currently selected. The visit will be deleted without prompting for confirmation.

Right-click menu option	Description
Sign In	This option is only available for a visit that is not active/not signed in. If the **Multiple Selection** checkbox is selected, multiple visits can be selected and signed in at once. Selecting this option does the same thing as clicking the [Sign In] button. If selected, the Sign In Visit(s) window is displayed. In this window, select whether to print disposable badges for the visitor that is being signed in.
Sign Out	This option is only available for a visit that is active/signed in. If the **Multiple Selection** checkbox is selected, multiple visits can be selected and signed out at once. Selecting this option does the same thing as clicking the [Sign Out] button. To use this feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the General Cardholder Options form of the Cardholder Options folder. For more information refer to Configure System-wide Visit Options in the Cardholder Options Folder chapter in the System Administration User Guide. When selected, the actual **Time out** for the visit is updated to the current date/time. If the visitor has an active badge, the deactivate date is updated and the badge status is set to the status setup that was selected on the General Cardholder Options form.
Find Cardholder	Opens the Cardholders folder and displays the cardholder record that is associated with the currently selected visit.
Find Visitor	Opens the Cardholders folder and displays the visitor record that is associated with the currently selected visit.
Refresh	Click this button to refresh the visits listed in the Visits listing window. When someone else makes changes in the database, you may need to click this button to see the changes. (Cardholder information is not automatically updated, but visit information is.)

Visits Folder Field Table

Visits Folder

Form Element	Type	Comment
Common form elements		
Visits listing window	display/selection	Displays the status, host, visitor, scheduled time in, scheduled time out, time in, time out, visit type and visit purpose for visit records.
Host name	display/text	Specifies the host for whom you want to display scheduled visits.
Visitor name	display/text	Specifies the visitor for whom you want to display scheduled visits.
Status	display	Displays the status of the visit. Choices include: • Scheduled - A visit that has a scheduled time in and scheduled time out that are both in the future • Late - A visit where the current date and time is after the scheduled time in • Overstayed - A visit where the current date and time is after the scheduled time out • Active - A visit that has been signed in and the scheduled time out has not yet been reached • Finished - A visit occurred in the past and has been signed out
Search	button	Allows you to search based on any field on any form in the Visits folder. The search results will be displayed in the Visits listing window.
Add	button	Allows you to add a visit record.
Modify	button	Allows you to modify a selected visit record. Multiple selection cannot be used when modifying visit records. If the **Multiple Selection** checkbox is selected and multiple visit records are selected, the [Modify] button will be grayed out.
Delete	button	Allows you to delete a selected visit record. If the **Multiple Selection** checkbox is selected, multiple visit records can be deleted at once. The visit(s) will be deleted without prompting for confirmation.
Print	button	Allows you to print a disposable badge. Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have “Visitor” selected for the **Class** and the **Disposable** checkbox must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.
Sign In	button	If selected, the Sign In Visit(s) window is displayed. In this window, select whether to print disposable badges for the visitor(s) that are being signed in. If the **Multiple Selection** checkbox is selected, multiple visit records can be signed in at once.

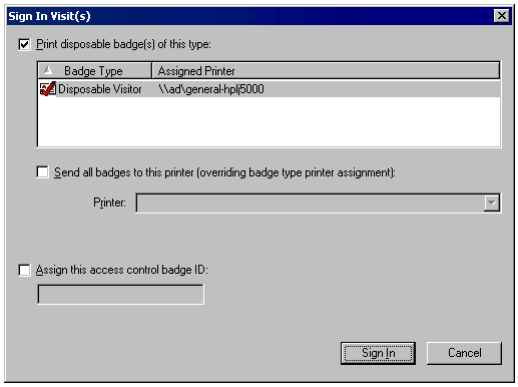
Visits Folder (Continued)

Form Element	Type	Comment
Sign Out	button	To use this feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the General Cardholder Options form of the Cardholder Options folder. For more information refer to the Cardholder Options Folder chapter in the System Administration User Guide. When selected, the actual **Time Out** for the visit is updated to the current date/time. If the visitor has an active badge, the deactivate date is updated and the badge status is set to the status setup that was selected on the General Cardholder Options form.
Multiple Selection	button	If selected, more than one entry in the listing window can be selected simultaneously. The changes made on this form will apply to all selected visits. This feature is primarily used for printing badges, signing in visits and signing out visits.

Sign In Visit(s) Window

This window is displays when:

- A visit is added in the Visits folder and the **Sign In Now** checkbox is selected on the Visit form.
- A visit record is selected in the Visit listing window in the Visits folder and the [Sign In] button is clicked.



Visits Folder - Sign In Visit(s) Window Field Table

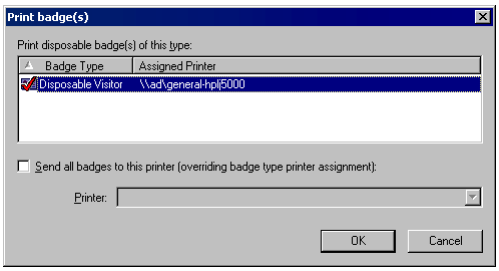
Form Element	Type	Comment
Print disposable badge(s) of this type	checkbox/display	• For these fields to be enabled, the **Allow disposable badge printing** checkbox on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. • Displays a list of disposable badge types that can be selected for the visit. • Only those badge types that are disposable are listed. • If you do not want to print a disposable badge for the visitor, deselect this checkbox.
Send all badges to this printer (overriding badge type printer assignment)	checkbox/drop-down list	• Select this checkbox to select an alternate printer • For these fields to be enabled, the **Choose alternate printer** checkbox on the Users Folder, Cardholder Permission Groups Form, Badge sub-tab must be selected. For more information refer to the Users Folder chapter in the System Administration or ID CredentialCenter users guide. • Selecting this checkbox overrides the printer assignments in the Printing/Encoding form of the Badge Types folder.

Visits Folder - Sign In Visit(s) Window Field Table (Continued)

Form Element	Type	Comment
Assign this access control badge ID	checkbox/numeric	• For these fields to be enabled, the **Allow access control badge assignment** checkbox on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. • The badge must already exist in the system • The existing badge's class must be "Visitor" • If the visitor already has an active access control badge (from a manual assignment or another visit), this field will automatically be populated with that ID. • If you do not want to assign an access control badge ID for the visitor, deselect this checkbox.
Sign In	push button	Signs in the visit using the options selected on the form.
Cancel	push button	Closes the Sign In Visit(s) window without signing in the visit.

Print Badge(s) Window

This window displays when the [Print] button is clicked on any form in the Visits folder.



Visits Folder - Print Badge(s) Window Field Table

Form Element	Type	Comment
Print disposable badge(s) of this type	display	• For this field to be enabled, the **Allow disposable badge printing** checkbox on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. • Displays a list of disposable badge types that can be selected for the visit. You must select a badge type and only one badge type can be selected. • Only those badge types that are disposable are listed.
Send all badges to this printer (overriding badge type printer assignment)	checkbox and drop-down list	• Select this checkbox to select an alternate printer. Chose the printer from the drop-down list. • For these fields to be enabled, the **Choose alternate printer** checkbox on the Users Folder, Cardholder Permission Groups Form, Badge sub-tab must be selected. For more information refer to the Users Folder chapter in the System Administration or ID CredentialCenter users guide. • Selecting this checkbox overrides the printer assignments in the Printing/Encoding form of the Badge Types folder.
OK	push button	Prints the disposable badge
Cancel	push button	Closes the Print Badge(s) window without printing the visit.

Visits Folder Procedures

The following procedures pertain to every form in the Visits folder unless otherwise noted.

Visit Search Capabilities

In search mode, you can search on any combination of fields in the Visits folder, including the Status search, Visit and Details forms. On the E-mail and Reports forms, you can only search for the host name or visitor name.

Comparison Operators

For text fields such as **Host name** and **Visitor name**, the default comparison is "begins with". The search results will include any records whose values begin with the characters that were entered. For example, when searching by last name, a filter of 'L' will find 'Lake', 'Lewis', etc. A filter of 'Lake' will find 'Lake', 'Lakeland', etc.

Search Text Fields for "Contains"

In addition to the default "begins with" searching for text fields, you can do a search for "contains" by prefixing the text with a percent sign ("%"). For example, typing "%mit" in the **Host name** field will find all people whose name contains the text "mit".

Search on Multiple Fields

When you search on multiple fields, the criteria is combined with "and". For example, typing "Lisa" in **Host name** field and "Lisa" in **Visitor name** field will find all visits where the host and the visitor's name are both "Lisa".

Search for All Visits to a Selected Cardholder

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Click [Search].
3. On any form in the Visits folder, click the [...] button to the right of the **Host name** drop-down list. The Select Host Wizard: Search form will open. For more information, refer to Select Host Wizard: Search Form on page 224.
   a. Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all cardholders.

   b. If a visitor is specified in the **Visitor name** field on the forms in the Visits folder and you wish to search for only cardholders who have been

visited by that visitor, select the **Previous hosts for current visitor only** checkbox.

c. Click [Next].

d. The Select Host Wizard: Select form opens. In the Cardholder listing window, select the cardholder you wish to add a visitor for. For more information, refer to Select Host Wizard: Select Form on page 226.

e. Click [Finish]. The cardholder's name will appear in the **Host name** field on the Visit form.

f. If you wish to locate all visits for the selected cardholder, click [OK] and the search results will be displayed in the Visits listing window. Alternately, you can specify additional search criteria.

Search for All Visits by a Selected Visitor

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Click [Search].
3. On any form in the Visits folder, click the [...] button to the right of the **Visitor name** field. The Select Visitor Wizard: Search form will be displayed. For more information, refer to Select Visitor Wizard: Search Form on page 227.

   a. Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all visitors.

---

   b. If a cardholder is specified in the **Host name** field on the forms in the Visits folder and you wish to only search for visitors who have visited that cardholder, select the **Previous visitors for current host only** checkbox.

   c. Click [Next].

   d. The Select Visitor Wizard: Select form will be displayed. For more information, refer to Select Visitor Wizard: Select Form on page 233.

   e. Select the visitor and click [Finish]. The visitor's name will appear in the **Visitor name** field on the Visit form.

   f. If you wish to locate all visits for the selected visitor, click [OK] and the search results will be displayed in the Visits listing window. Alternately, you can specify additional search criteria.

Search for Scheduled, Active or Finished Visits

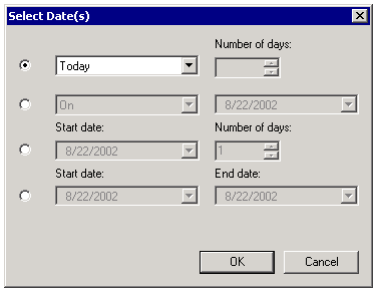
1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Click the Status search tab.
3. Click [Search].
4. In the Search for visits that are any combination of these section, select that status you wish to search for.
   a. To search for scheduled visits, select the **Scheduled, future** checkbox.
      - If you wish to search for visits that are scheduled to begin in a specified number of minutes, hours or days, select the **Starting within** checkbox and then specify the number of minutes, hours or days.
      - By default, scheduled visits that are late getting started will also be searched for. If you do not want to search for scheduled visits that are late, deselect the **Scheduled, late** checkbox.

   b. To search for active visits, select the **Active** checkbox.
      - If you wish to search for visits that are scheduled to end within a specified number of minutes, hours or days, select the **Ending within checkbox** and then specify the number of minutes, hours or days.
      - By default, active visits that are late being signed out (overstayed) will also be searched for. If you do not want to search for active visits that are overstayed, deselect the **Active, overstayed** checkbox.

   c. To search for finished visits, select the **Finished** checkbox.
5. The refresh rate is how often the database is queried to see if it has changed. This setting is stored on a per user basis. Select the refresh option that meets your needs.
   - If the **Use system default rate** checkbox is selected, the rate that is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options folder will be used.
   - If the **Use system default rate** checkbox is not selected, type the number of minutes you wish to elapse between the times that the database is queried for changes in the **Refresh rate (minutes)** field.
6. Click [OK]. The visit records that meet the search criteria will be displayed in the Visits listing window.

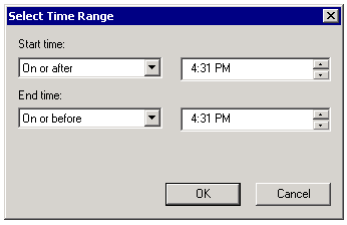
Search for All Visits for a Specific Date or Time

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Click the Visit tab.
3. Click [Search].
4. To search for the date of a specific scheduled time in, click the [...] button to the right of the **Scheduled time in** field.
   a. The Select Date(s) window opens.



   b. Select a search option. Choices include:
      - Today, previous number of days or next number of days
      - On a specified date
      - Starting on a specified date and including a specified number of days from that date
      - Starting on a specified date and ending on a specified date
   c. Click [OK].
   d. The code for the search criteria that you just specified will be displayed in the **Scheduled time in** field.
5. To search for the time of a specific scheduled time in, click the [...] button to the right of the time field, as shown.

   a. The Select Time Range window opens.



   b. In the **Start time** drop-down list, select whether the visit's start time is on or after the specified time, after the specified time or has no specified time. You can change the time by clicking in the field and typing new

values or by using the spin buttons. The hour, minute and time of day are all adjusted individually.

c. In the **End time** drop-down list, select whether the visit's end time is on or after the specified time, after the specified time or has no specified time. You can change the time by clicking in the field and typing new values or by using the spin buttons. The hour, minute and time of day are all adjusted individually.

d. Click [OK].

6. Click [OK]. The visit records that meet the search criteria will be displayed in the Visits listing window.

7. To search for a scheduled time out, time in or time out, repeat the same process described in steps 4 - 6, except use the [...] buttons to the left of whichever time you are searching for.

Retrieve the Most Recent Visit Search Results

1. Click [Search].
2. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
3. If you want, modify your search criteria.
4. Click [OK].
5. B.A.S.I.S. retrieves and displays the matching record(s) in the Visits listing window.

Find a Cardholder or Visitor Associated with a Visit

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Locate the visit record that you wish to find the visitor or cardholder for.
3. Right-click on the visit record.
   - If you wish to view the cardholder record, select **Find Cardholder**.
   - If you wish to view the visitor record, select **Find Visitor**.
4. The record of the corresponding cardholder or visitor will be displayed in the Cardholder or Visitor window.

Add a Visit Record

To add a visit, information about the visit needs to be entered on the Visit, Details and E-mail forms in the Visits folder; it does not matter which form you start with. When the Visits folder opens, the Visit form displays by default, so this procedure begins on that form.

Note: This procedure does not apply to view/edit only workstations.

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. On the Visit form:
   a. A new visit record can either be based on an existing visit record or it can be an entirely new record.
      - To create a record based on an existing visit record, select a visit record in the Visits listing window, then click [Add]. The fields prepopulate with the information from the selected visit. You can select new values for any field.
      - To create a record that is not based on an existing visit record, make sure that no visit record is selected in the Visits listing window, then click [Add]. The fields will be blank to begin with.

Note: Steps b and c can be done in either order.

   b. Click the [...] button to the right of the **Host name** drop-down list. The Select Host Wizard: Search form opens. For more information, refer to Select Host Wizard: Search Form on page 224.
      1) Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all cardholders.

      2) If a visitor is specified and you wish to search for only cardholders who have been visited by that visitor, select the **Previous hosts for current visitor only** checkbox.
      3) Click [Next].
      4) The Select Host Wizard: Select form opens. In the Cardholder listing window, select the cardholder you wish to add a visitor for. For more information, refer to Select Host Wizard: Select Form on page 226.
      5) Click the [Finish]. The cardholder's name appears in the **Host name** field on the Visit form.
   c. Click the [...] button to the right of the **Visitor name** field. The Select Visitor Wizard: Search form displays.
      1) Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all visitors.

2) If a cardholder is specified and you wish to only search for visitors who have visited that cardholder, select the **Previous visitors for current host only** checkbox.

3) Click the [Next].

4) The Select Visitor Wizard: Select or Add form displays. If the Visitor is listed below, select the visitor and click [Finish]. The visitor's name appears in the **Visitor name** field on the Visit form. If the Visitor is not listed below, select the **Create new visitor** radio button and click [Next]. The Select Visitor Wizard: Add form displays. Enter the new visitor's information and click [Finish].

Note: For a detailed description of the Select Visitor Wizard: Select or Add form refer to Select Visitor Wizard: Select or Add Form on page 229.

---

d. In the **Scheduled time in** fields, specify the date and time the visit will begin. You can either type the values or select them.

Note: If the **Sign In Now** checkbox is selected, these fields will be grayed out.

---

e. In the **Scheduled time out** fields, specify the date and time the visit will end. You can either type the values or select them.

f. Select the **Sign In Now** checkbox if the visit is starting immediately. If you select this option, the **Scheduled time in** fields will become grayed out and the date and time when you click the [OK] button will be assigned as the visit's **Time in**.

3. Click the Details tab. For a detailed description of the Details form refer to Details Form on page 217. On the Details form:

a. In the **Type** drop-down list, select the type of visit.

Note: Types of visits must first be configured in the List Builder, which is displayed in System Administration or ID CredentialCenter by selecting the **Administration** menu, then selecting **List Builder**.

---

b. In the **Purpose** field, type the reason for the visitor's visit.

4. You may wish to send e-mail notifications to all parties that require information about a scheduled visit. For a detailed description of the E-mail form refer to E-mail Form on page 218. To set up e-mail notifications, click the E-mail tab. On the E-mail form:

Note: For an e-mail to be sent, the **Allow e-mail notification** checkbox on the Visits form in the Cardholder Options folder must be selected.

---

a. In the Include section, verify the **Default Recipients** checkbox is selected as long as you wish to send e-mail messages to the default

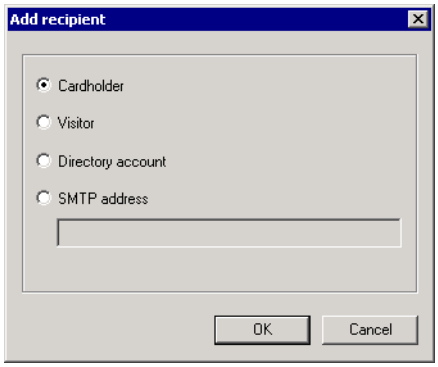
recipients. The default recipients are configured in the following locations:

- On segmented systems, select **Administration** > **Segments**, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can view or modify the default recipients.
- On nonsegmented systems, select **Administration** > **System Options**, then click the Visits tab. On the Visits tab, you can view or modify the default recipients.

b. Select the **Cardholder for this visit** checkbox if you wish to have an e-mail sent to the cardholder for this visit.

c. Select the **Visitor for this visit** checkbox if you wish to have an e-mail sent to the visitor for this visit.

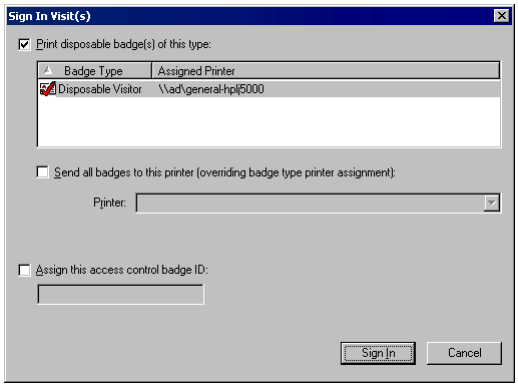
d. Click [Add] if you wish to add another recipient. The Add recipient window displays. You may add a cardholder, visitor, directory account or SMTP address.



- If you select the **Cardholder** radio button and click [OK], the Select Host Wizard: Search form displays. For a detailed description of the Select Host Wizard: Search form refer to Select Host Wizard: Search Form on page 224.
- If you select the **Visitor** radio button and click [OK], the Select Visitor Wizard: Search form displays. For a detailed description of the Select Visitor Wizard: Search form refer to Select Visitor Wizard: Search Form on page 227.
- If you select the **Directory account** radio button and click [OK], the Select Account window displays.
- If you select the **SMTP address** radio button, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.

5. Click the [OK].
6. If the **Sign in now** checkbox was selected, proceed to step 7. If the **Sign in now** checkbox was not selected, the visit will be added. The value for the **Time In** column for the visit will remain blank and the visit can be signed in later when it actually occurs.
7. If none of the **Allow disposable badge printing**, **Allow access control badge assignment** and **Allow e-mail notification** checkboxes are checked

on the Visits form in the Cardholder Options folder, the visit will be signed in. If any of those options are selected, the Sign In Visit(s) window displays.



8. The **Print disposable badge(s) of this type** checkbox and listing window are enabled if the **Allow disposable badge printing** checkbox is selected on the Visits form in the Cardholder Options folder.

   - If enabled, you can print a disposable badge for the user by selecting the **Print disposable badge(s) of this type** checkbox, then selecting a disposable badge type to be assigned and printed.

Note: Disposable badge types are configured in the Badge Types folder in System Administration. For a badge type to be used to print disposable badges, it must have "Visitor" selected for the **Class** and the **Disposable** checkbox must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

   - If the checkbox is deselected, the system will not print a disposable badge.

9. To override the badge type printer assignment select the **Send all badges to this printer (overriding badge type printer assignment)** checkbox and select the printer from the drop-down list. This checkbox and drop-down list

are enabled if the **Print disposable badge(s) of this type** checkbox is selected and the user has the correct permissions.

10. The **Assign this access control badge ID** checkbox and field are enabled if the **Allow access control badge assignment** checkbox is selected on the Visits form in the Cardholder Options folder in System Administration.
    - If enabled, you can select the **Assign this access control badge ID** checkbox and then type the number of an existing badge that has the class "Visitor" in the field or leave the field blank.
    - If the visitor already has an active access control badge (from manual assignment or another visit), this field will automatically be filled in with that ID.
    - If the checkbox is deselected, the system will not attempt to assign an access control badge ID.
11. Click the [Sign In]. The visit will be added, the **Time In** field will be updated to the current date and time and any access control badge assigned will become active.

Modify a Visit Record

Note: This procedure does not apply to view only workstations.

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Locate the visit record you want to change and select it in the Visits listing window.

Note: Multiple selection cannot be used when modifying visits.

3. Click the [Modify].
4. Make the changes you want to the record. Changes can be made on any tab in the Visits folder.
5. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Visit Record

Note: This procedure does not apply to view/edit only workstations.

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. In the Visits listing window select the visit record you want to delete.

Note: To select multiple visit records select the **Multiple Selection** checkbox.

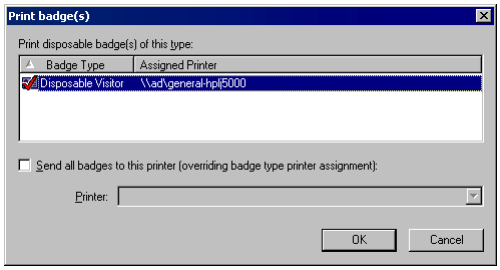
3. Click the [Delete].
4. Click the [OK]. The visit(s) will be deleted without confirmation.

Print a Badge for a Visitor

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. In the Visits listing window select the visit record you want to print.

Note: To select multiple visit records select the **Multiple Selection** checkbox.

3. On any form in the Visits folder, click [Print].
4. The Print badge(s) window displays. In the **Print disposable badge(s) of this type** listing window select the type of badge to print.



Note: Disposable badge types are configured in the Badge Types folder in System Administration and must have "Visitor" selected for the **Class** and the **Disposable** checkbox selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

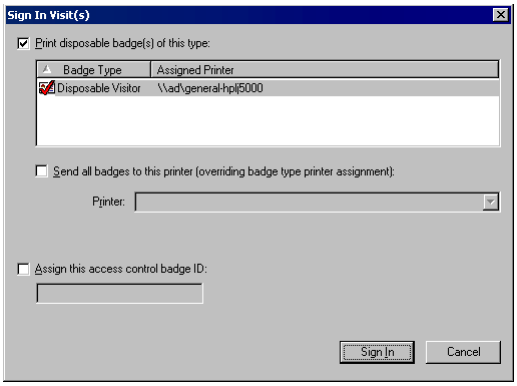
5. To select an alternate printer select the **Send all badges to this printer (overriding badge type printer assignment)** checkbox and choose a printer from the drop-down list. This checkbox and drop-down list are enabled if the user has the correct permissions.
6. Click the [OK].

Sign in a Previously Scheduled Visit

Note: This procedure does not apply to view only workstations.

Each visit has a time that it is scheduled to begin. When the visitor arrives and the visit actually begins, the visit should be "signed in". When a visit is signed in, the actual **Time In** of the visitor is updated to the current date and time and any access control badge that the visitor is issued is activated. A visit can be signed in immediately after it is added or it can be signed in later. To sign in a visit:

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. In the Visits listing window, locate and select the visit record you wish to sign in. Click the [Sign In].
3. If none of the **Allow disposable badge printing**, **Allow access control badge assignment** and **Allow e-mail notification** checkboxes are checked on the Visits form in the Cardholder Options folder, the visit will be signed in. If any of those options are selected, the Sign In Visit(s) window displays.



4. The **Print disposable badge(s) of this type** checkbox and listing window are enabled if the **Allow disposable badge printing** checkbox is selected on the Visits form in the Cardholder Options folder.
   - If enabled, you can print a disposable badge for the user by selecting the **Print disposable badge(s) of this type** checkbox, then selecting a disposable badge type to be assigned and printed.

Note: Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have "Visitor" selected for the **Class** and the **Disposable** checkbox must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

   - If the checkbox is deselected, the system will not print a disposable badge.
5. To override the badge type printer assignment select the **Send all badges to this printer (overriding badge type printer assignment)** checkbox and select the printer from the drop-down list. This checkbox and drop-down list

are enabled if the **Print disposable badge(s) of this type** checkbox is selected and the user has the correct permissions.

6. The **Assign this access control badge ID** checkbox and field are enabled if the **Allow access control badge assignment** checkbox is selected on the Visits form in the Cardholder Options folder.
   - If enabled, you can select the **Assign this access control badge ID** checkbox and then type the number of an existing badge that has the class "Visitor" in the field or leave the field blank.
   - If the visitor already has an active access control badge (from manual assignment or another visit), this field will automatically be filled in with that ID.
   - If the checkbox is deselected, the system will not attempt to assign an access control badge ID.
7. Click the [Sign In]. The visit will be added, the **Time In** field will be updated to the current date and time and any access control badge assigned will become active.

Sign Out a Visit

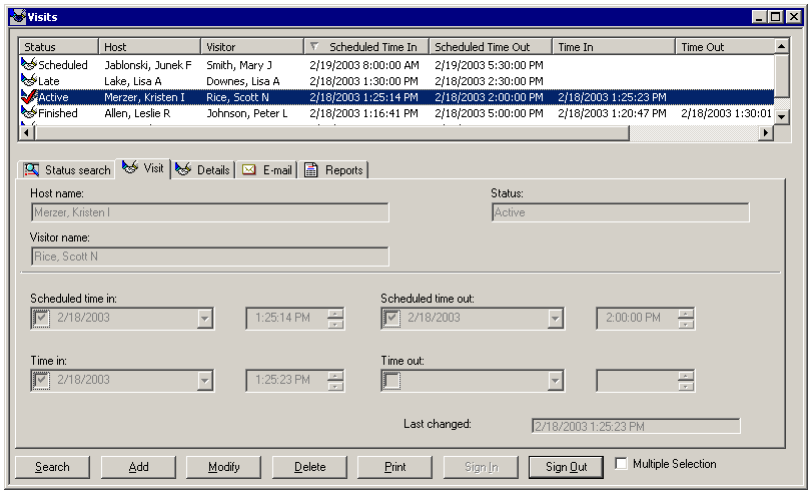
Note: This procedure does not apply to view only workstations.

Each visit has a time that it is scheduled to end. When the visitor leaves and the visit actually ends, the visit should be "signed out". When a visit is signed out, the actual **Time Out** of the visitor is updated to the current date and time and any access control badge that the visitor is issued is deactivated.

To use the Sign Out feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the Visits form in the Cardholder Options folder. For more information refer to "Configure System-wide Visit Options" in the Cardholder Options Folder in the System Administration User Guide.

1. Select **Visits** from the **View** menu. The Visits folder opens.
2. Locate the active visit record that needs to be signed out.
3. In the Visits listing window, select the active visit that you want to sign out by clicking on it.
4. Click the [Sign Out].
5. The message "Are you sure you wish to sign out the selected visit(s)? This will also deactivate any badges the visitors have." will be displayed. Click [Yes] to complete the sign out. The **Time out** will be updated to the current date/time. If the visitor has an active badge, the deactivate date will be updated and the badge status will be set to the status setup that was selected on the Cardholder Options form. The signed out visit will appear in the Visits listing window.

Visit Form



Visit Form Overview

The Visit form is displayed by default when the Visits folder opens. It is used to:

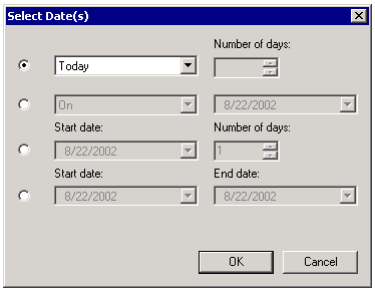
- Add or modify visits
- Display visit records for a selected date range
- Search for visit records based on the scheduled time in, scheduled time out, time in, time out or date and time last changed

Visit Form Field Table

Form Element	Type	Comment
Scheduled time in	drop-down listbox	Select the date and time that the visit is expected to start.
Time in	drop-down listbox	When a visit is signed in, the visit's **Time in** gets updated to the current date and time.
Scheduled time out	drop-down list	Select the date and time that the visit is expected to end.
Time out	drop-down list	When a visit is signed out, the visit's **Time out** gets updated to the current date and time.
Last changed	display	Indicates the date and time on which this visit record was last modified and saved. This date and time are only updated when visit information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Select Date(s) Window

This window is only displayed when the Visit form in the Visits folder is in Search mode. In Search mode, click the [...] to the right of the first **Scheduled time in**, **Time in**, **Scheduled time out** or **Time out** field.

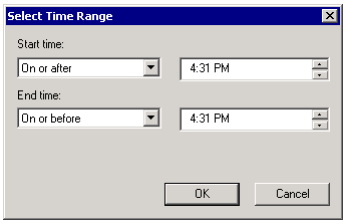


Visit Form - Select Date(s) Window Field Table

Form Element	Type	Comment
Day	radio button/drop-down listbox/spin buttons	Used when searching for a scheduled time in, time in, scheduled time out or time out. Selects visits that occurred today, on a previous number of days or on a specified number of days in the future.
Specific Date	radio button/drop-down listboxes	Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects visits that occurred on a specified date. Choices include on, on or after, after, on or before or before a specified date.
Number of Days After a Date	radio button/drop-down listbox/spin buttons	Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects visits between a specified start date and a specified number of days after the start date.
Between Two Dates	radio button/drop-down listboxes	Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects all visits that occurred between the specified Start date and the End date.
OK	push button	Enters the code for the selected search criteria in the respective field on the Visit form in the Visits folder.
Cancel	push button	Closes the Select Date(s) window without selecting a date search criteria.

Select Time Range Window

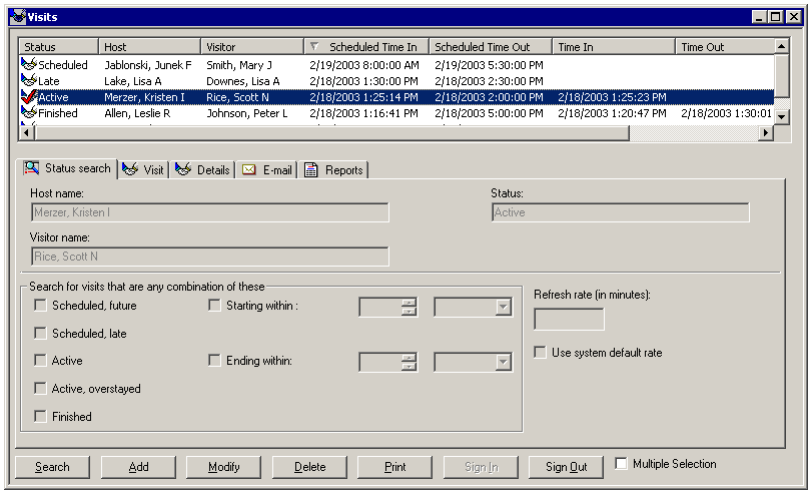
This window is only displayed when the Visit form in the Visits folder is in Search mode. In Search mode, click the [...] to the right of the second **Scheduled time in**, **Time in**, **Scheduled time out** or **Time out** field.



Visit Form - Select Time Range Window Field Table

Form Element	Type	Comment
Start time	drop-down listbox/ spin buttons	Used when searching for the time portion of a scheduled time in, time in, scheduled time out or time out. Allows you to search for visits that start on or after or after a specified time. If “None” is selected, no time restraints are put on the visit records that are returned. (Visits that started at any time on the specified date will be returned.)
End time	drop-down listbox/ spin buttons	Used when searching for the time portion of a scheduled time in, time in, scheduled time out or time out. Allows you to search for visits that end on or before or before a specified time. If “None” is selected, no time restraints are put on the visit records that are returned. (Visits that ended at any time on the specified date will be returned.)
OK	push button	Enters the code for the selected search criteria in the respective field on the Visit form in the Visits folder.
Cancel	push button	Closes the Select Time Range window without selecting a time search criteria.

Status Search Form



Status Search Form Overview

The Status Search form is only enabled when the [Search] button is clicked. It is used to:

- Search for Visits that meet a specified criteria (scheduled in the future, scheduled but late, active, finished, etc.)
- Set the refresh rate

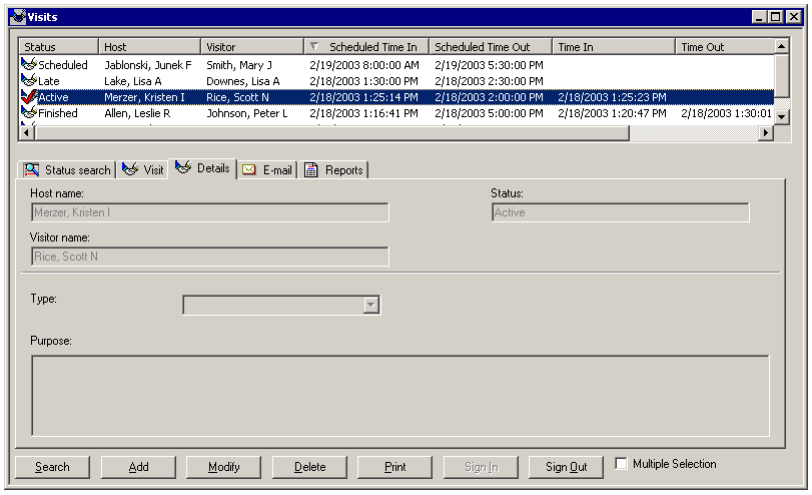
Status Search Form Field Table

Form Element	Type	Comment
Scheduled, future	checkbox	If selected, the search will find visits that are scheduled in the future, i.e., have a scheduled time in that is in the future and have not been signed in yet
Starting within	checkbox/spin-buttons/drop-down list	Enabled for selection only when the **Scheduled, future** checkbox is selected. If selected, specify the number of hours, days or minutes that the visit is scheduled to begin in. For example, you can search for all visits that are scheduled to begin within the next two days.
Scheduled, late	checkbox	If selected, the search will find visits that are late, i.e., have a scheduled time in that is in the past and have not been signed in yet
Active	checkbox	If selected, the search will find all visits that are currently signed in and have not been signed out yet
Ending within	checkbox/spin-buttons/drop-down list	Enabled for selection only when the **Active** checkbox is selected. If selected, specify the number of hours, days or minutes that the visit is scheduled to end in. For example, you can search for all visits that are scheduled to end within the next two days.

Status Search Form Field Table (Continued)

Form Element	Type	Comment
Active, overstayed	checkbox	If selected, the search will find all visits that are currently signed in where the current date and time is after the scheduled time out. For example, a visitor that was supposed to leave at 3 p.m., but is still visiting at 5 p.m.
Finished	checkbox	If selected, the search will locate visits that occurred in the past.
Refresh rate (in minutes)	numeric	The refresh rate is how often the database is queried to see if it has changed. The refresh rate is stored on a per user basis and only applies when searching based on a status (i.e., the “Scheduled, future”, “Scheduled, late”, “Active”, “Active, overstayed” or “Finished” status) on the Status search form in the Visits folder. The default value is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options form. A custom refresh rate can be specified as long as the **Use system default rate** checkbox is not selected.
Use system default rate	checkbox	If selected, the system default rate will be used when refreshing. The system default rate is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options folder. If not selected, a custom refresh rate can be specified in the **Refresh rate (in minutes)** field.

Details Form



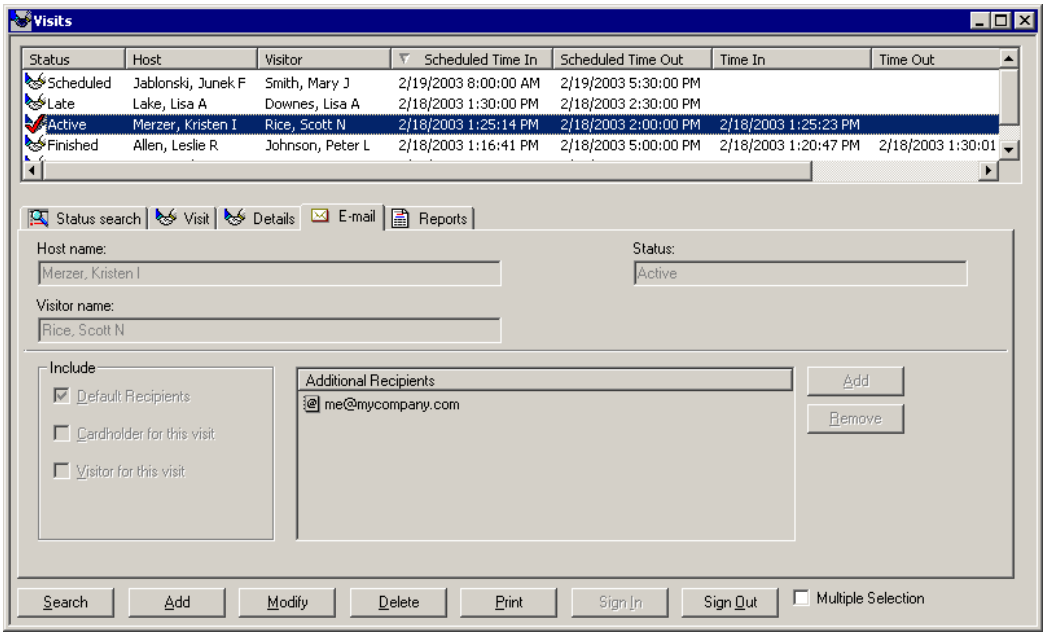
Details Form Overview

The Details form is a user-defined form that has been created for you. This form can be modified or even deleted using FormsDesigner. By default, the form contains the type and purpose of the visit.

Details Form Field Table

Form Element	Type	Comment
Type	drop-down listbox	Select the type of visit. **Note:** Types of visits must first be configured in the List Builder, which is displayed by selecting the **Administration** menu, then selecting **List Builder**. For more information refer to the List Builder Folder chapter in the System Administration User Guide
Purpose	drop-down listbox	Type the reason why the visitor is visiting the cardholder.

E-mail Form



E-mail Form Overview

The E-mail form is used to specify e-mail addresses and pager numbers that are automatically notified of visits. You can:

- Add a recipient
- Remove a recipient
- Specify whether to e-mail the default recipients, the cardholder being visited and/or the visitor

E-mail Form Field Table

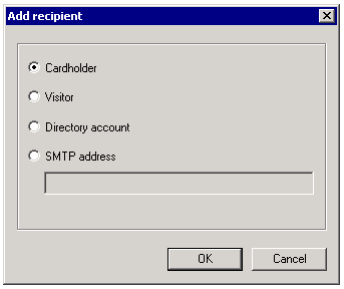
Form Element	Type	Comment
Default Recipients	checkbox	Select this checkbox if you wish to send e-mail messages to the default recipients. • On segmented systems, select **Administration** > **Segments**, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can add or remove recipients. These recipients will be collectively considered the “Default Recipients” on the E-mail form in the Visits folder. • On non segmented systems, select **Administration** > **System Options**, then click the Visits tab. On the Visits tab, you can view or modify the default recipients. Whether this checkbox is selected by default when a new visit is added is determined by the **Include default recipients by default** checkbox on the Visits form in the Cardholder Options folder.

E-mail Form Field Table (Continued)

Form Element	Type	Comment
Cardholder for this visit	checkbox	Select this checkbox if you wish to have an e-mail sent to the cardholder for this visit. Whether this checkbox is selected by default when a new visit is added is determined by the **Include host's e-mail by default** checkbox on the Visits form in the Cardholder Options folder.
Visitor for this visit	checkbox	Select this checkbox if you wish to have an e-mail sent to the visitor for this visit. Whether this checkbox is selected by default when a new visit is added is determined by the **Include visitor's e-mail by default** checkbox on the Visits form in the Cardholder Options folder.
Additional Recipients listing window	display/selection	Displays the e-mail addresses that will receive e-mail notification of visits. **Note:** The addresses for the default recipients are not displayed in this listing window.
Add	button	Click this button if you wish to add another recipient. The Add recipient window is displayed. You may add a cardholder, visitor, directory account or SMTP address. • If you select the **Cardholder** radio button and click [OK], the Select Host Wizard: Search form is displayed. • If you select the **Visitor** radio button and click [OK], the Select Visitor Wizard: Search form is displayed. • If you select the **Directory account** radio button and click [OK], the Select Account window is displayed. • If you select the **SMTP address radio button**, type the SMTP address, then click [OK]. An example of an SMTP address is "joesmith@company.com".
Remove	button	Removes the selected recipient from the list of recipients that will receive notification of visits.

Add Recipient Window

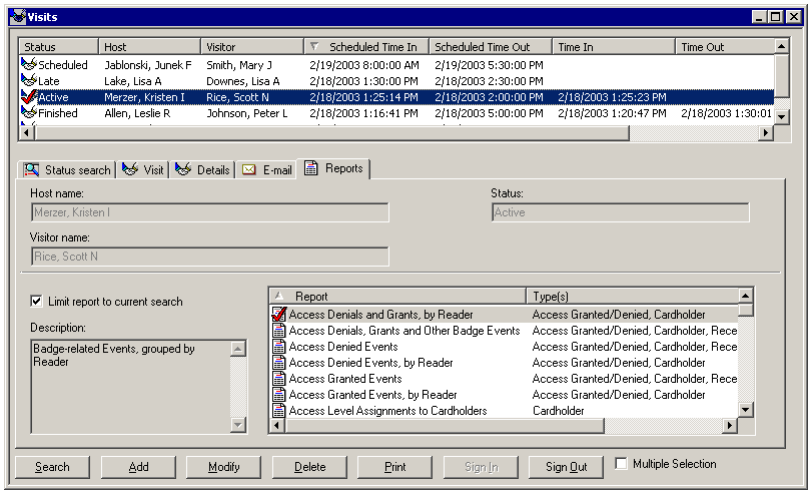
This window is displayed when the E-mail form in the Visits folder is in Add or Modify mode and the [Add] button to the right of the Additional Recipients listing window is clicked.



E-mail Form - Add Recipient Window Field Table

Form Element	Type	Comment
Cardholder	radio button	The Select Host Wizard: Search form is displayed, which allows you to add a cardholder as an e-mail recipient. For more information, refer to Select Host Wizard: Search Form on page 224.
Visitor	radio button	The Select Visitor Wizard: Search form is displayed, which allows you to add a visitor as an e-mail recipient.
Directory account	radio button	The Select Account window is displayed, which allows you to add a directory account as an e-mail recipient.
SMTP address	radio button	Type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.
OK	push button	• If you selected the **Cardholder** radio button, the Select Host Wizard: Search form is displayed. For more information, refer to Select Host Wizard: Search Form on page 224. • If you selected the **Visitor** radio button, the Select Visitor Wizard: Search form is displayed. For more information, refer to Select Visitor Wizard: Search Form on page 227. • If you selected the **Directory account** radio button, the Select Account window is displayed. • If you selected the **SMTP address** radio button and typed an SMTP address, the address will be added to the Additional Recipients listing window.
Cancel	push button	Closes the Add recipient window without adding a recipient.

Reports Form



Reports Form Overview

The Reports form shows only visit-related reports. For a specific list of visit-related reports refer to Appendix C: Visit-Related Reports on page 243. On the Reports form you can:

- Search for a cardholder
- Search for a visitor
- Generate a report

Reports Form Field Table

Form Element	Type	Comment
Limit report to current search	checkbox	If selected, the report will only include those records that match the rest of the search criteria specified on any form in the Visits folder. If not selected, the report will include all records for the selected report type.
Description	display	A brief description of the report contents.
Report listing window	display/selection	Lists currently defined reports of the type(s) selected in the Report listing window.

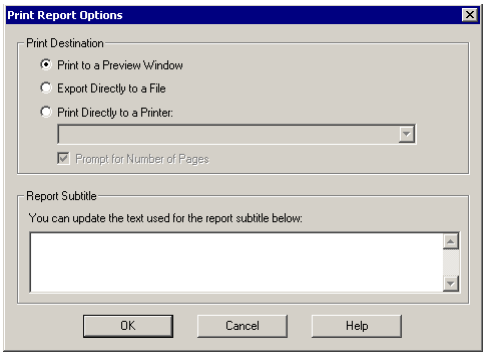
Reports Form Procedures

Run a Visit Report from the Visits Folder

A visit report can be generated for either a defined search criteria or for all visits.

Note: This procedure does not apply to view only workstations.

1. If you wish to generate a visit report that searches through all visit records not just those that match a search criteria, proceed to step 2. To generate a visit report based on a search criteria:
   a. Select **Visits** from the **View** menu. The Visits folder opens.
   b. In the Visits folder, click [Search].
   c. Run the search that you wish to print a report for. For more information on searching refer to the following:
      - Visit Search Capabilities on page 199
      - Search for All Visits to a Selected Cardholder on page 199
      - Search for All Visits by a Selected Visitor on page 200
      - Search for Scheduled, Active or Finished Visits on page 201
      - Search for All Visits for a Specific Date or Time on page 202
      - Retrieve the Most Recent Visit Search Results on page 203
   d. Click the Reports tab.
   e. Select the **Limit report to current search** checkbox.
   f. Proceed to step 3.
2. To generate a visit report that searches through all visits:
   a. Select **Visits** from the **View** menu. The Visits folder opens.
   b. In the Reports listing window, select the type of report you wish to print. For more information, refer to Appendix C: Visit-Related Reports on page 243.
   c. Proceed to step 3.
3. Click the [Print]. The Print Report Options window opens.



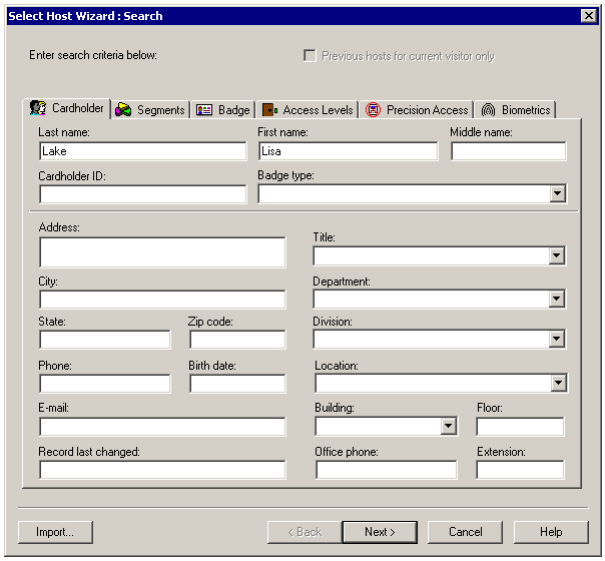
4. In the Print Destination section, select whether to print to a preview window, export directly to a file or print directly to a printer.
5. If you selected **Print Directly to a Printer** in the Print Destination section, select a printer in the drop-down list and choose whether to **Prompt for Number of Pages**.

6. In the Report Subtitle section, type the report subtitle. If the **Limit report to current search** checkbox is selected, the search criteria will be listed in the Report Subtitle section by default. The subtitle will be displayed below the report title on the report.
7. Click the [OK]. The options selected in the Print Destination section will determine where the report is sent.

Select Host Wizard: Search Form

Note: If the FormsDesigner application has been used to customize your cardholder data, the elements on your Select Host Wizard: Search form will be different. The default fields are pictured below.

This form is displayed when the [Search] button in the Visits folder is clicked and then the [...] button to the right of the **Host name** field is clicked.



Select Host Wizard: Search Form Overview

This form is used to enter search criteria that will allow you to locate a specific cardholder.

Visits Folder - Select Host Wizard: Search Form

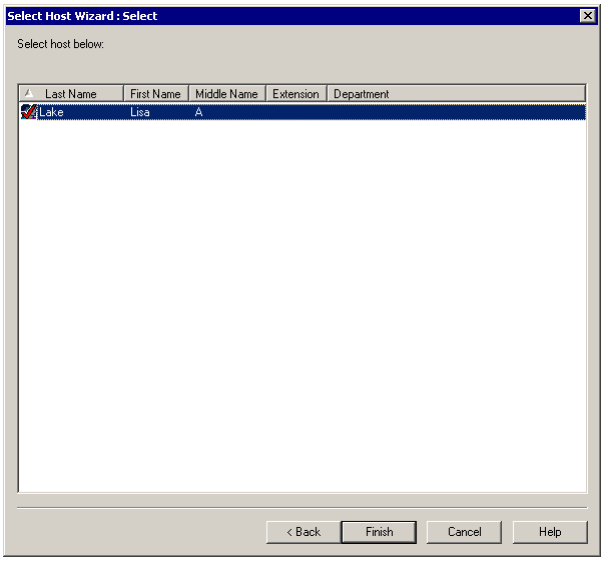
Form Element	Type	Comment
Previous hosts for current visitor only	checkbox	This checkbox is only enabled when a visitor has been selected and a cardholder is being searched for. If selected, only those cardholders who have previously been visited by the selected visitor will be displayed on the Select Visitor: Select or Add form.
Last name	text	Indicates cardholder's last name.
First name	text	Indicates cardholder's first name.
Middle name	text	Indicates cardholder's middle name.
Cardholder ID	numeric	Indicates a cardholder's ID, which is most commonly their Social Security Number. The cardholder ID must be a numeric value.

Visits Folder - Select Host Wizard: Search Form (Continued)

Form Element	Type	Comment
Badge type	drop-down list	Selects which of the cardholder's badges (if he or she has more than one) is to be the active one.
User-defined fields		All fields below the line on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your cardholder data.
Back	push button	This button is not used.
Next	push button	The wizard will proceed to the Select Host Wizard: Select form.
Cancel	push button	Closes the window without locating a cardholder and returns you to the Visit form in the Visits folder.
Help	push button	Displays online help for this topic
Import	push button	Displays the Select Import Source window, which allows you to select a device to import cardholder data from, such as a business card scanner

Select Host Wizard: Select Form

This form is displayed when the [Next] button on the Select Host Wizard: Search form is clicked.



Select Host Wizard: Select Form Overview

This form is used to select a cardholder record from those that matched the specified search criteria. The columns displayed are configured on the Cardholder Search Results form in the Cardholder Options folder. For more information refer to the Segments Folder chapter in the System Administration User Guide.

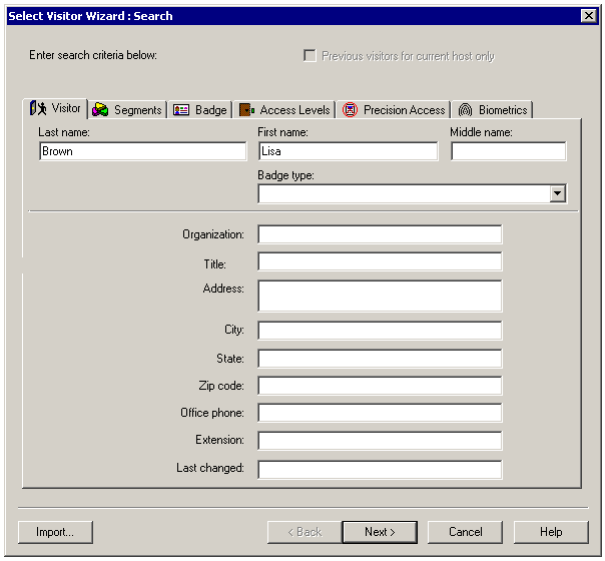
Visits Folder - Select Host Wizard: Select Form

Form Element	Type	Comment
Cardholder listing window	display	A list of cardholder records that match the search criteria specified on the Select Host Wizard: Search form are displayed. **Note:** The fields that are displayed in columns are set on the Cardholder Search Results Lists form in the Cardholder Options folder.
Back	push button	Returns to the Select Host Wizard: Search form.
Finish	push button	Completes the wizard. The selected cardholder's name will be displayed in the **Host name** field.
Cancel	push button	Closes the window without selecting a cardholder and returns you to the Visit form in the Visits folder.
Help	push button	Displays online help for this topic

Select Visitor Wizard: Search Form

Note: If the FormsDesigner application has been used to customize your visitor data, the elements on your Select Visitor Wizard: Search form will be different. The default fields are pictured below.

This form is displayed when the [...] button to the right of the **Visitor name** drop-down list on the Visit form is clicked.



Select Visitor Wizard: Search Form Overview

This form is used to locate visitor records that match the specified search criteria.

Visits Folder - Select Visitor Wizard: Search Form

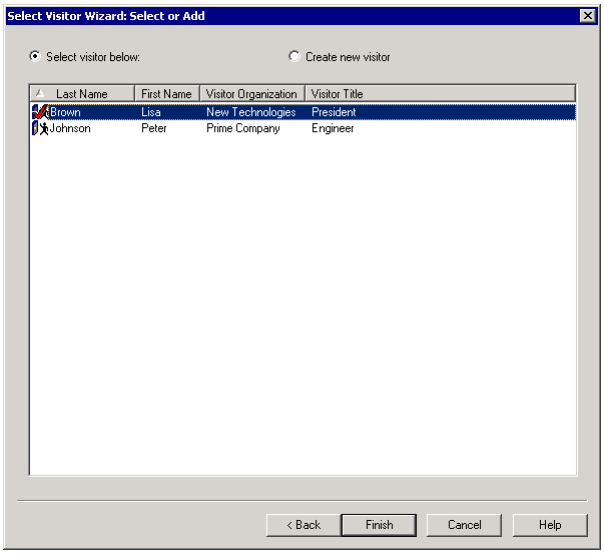
Form Element	Type	Comment
Previous visitors for current host only	checkbox	This checkbox is only enabled when a cardholder has been selected and a visitor is being searched for. If selected, only those visitors who have previously visited the selected cardholder will be displayed on the Select Visitor: Select or Add form.
Last name	text	Indicates visitor's last name.
First name	text	Indicates visitor's first name.
Middle name	text	Indicates visitor's middle name.
Badge type	drop-down listbox	Indicates the visitor's badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.

Visits Folder - Select Visitor Wizard: Search Form (Continued)

Form Element	Type	Comment
User-defined fields		All fields below the horizontal line on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.
Back	push button	This button is not used.
Next	push button	The wizard will proceed to the Select Visitor Wizard: Select or Add form.
Cancel	push button	Closes the window without locating a visitor and returns you to the Visit form in the Visits folder.
Import	push button	Displays the Select Import Source window, which allows you to select a device to import visitor data from, such as a business card scanner
Help	push button	Displays online help for this topic

Select Visitor Wizard: Select or Add Form

This form is displayed when the [Next] button on the Select Visitor Wizard: Search form is clicked.



Select Visitor Wizard: Select or Add Form Overview

This form is displayed when adding a visit. From this form, you can:

- Search for visitor records that match the specified search criteria.
- Add a new visitor record.

Visits Folder - Select Visitor Wizard: Select or Add Form

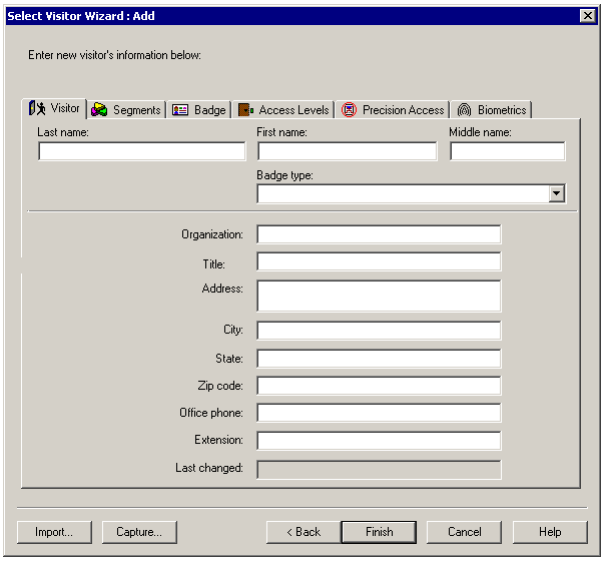
Form Element	Type	Comment
Select visitor below	radio button	Select this option if the visitor you need to add a visit for is listed below in the Visitor listing window. If you select this option, also select a visitor in the Visitor listing window below.
Create new visitor	radio button	Select this option if the visitor you need to add a visit for is not listed in the Visitor listing window. If you select this option, the [Finish] button will be replaced with a [Next] button. When the [Next] button is clicked, the Select Visitor Wizard: Add form will be displayed, on which you can add a new visitor.

Visits Folder - Select Visitor Wizard: Select or Add Form (Continued)

Form Element	Type	Comment
Visitor listing window	display	A list of visitor records that match the search criteria specified on the Select Visitor Wizard: Search form are displayed. **Note:** The fields that are displayed in columns are set on the Visitor Search Results Lists form in the Cardholder Options folder.
Back	push button	Returns to the Select Visitor Wizard: Search form.
Finish	push button	This button is displayed only if **Select visitor below** is selected. Click this button to complete the wizard. The selected visitor's name will be displayed in the **Visitor name** field. If **Create new visitor** is selected, the [Finish] button is replaced by a [Next] button.
Cancel	push button	Closes the window without selecting a visitor and returns you to the Visit form in the Visits folder.
Help	push button	Displays online help for this topic

Select Visitor Wizard: Add Form

This form is displayed when **Create new visitor** is selected and the [Next] button is clicked on the Select Visitor Wizard: Select or Add form.



Select Visitor Wizard: Add Form Overview

This form allows you to:

- Add a new visitor record
- Capture photographic information such as a photo, signature or biometric data for a visitor
- Import visitor data from a business card scanner or other similar device

Visits Folder - Select Visitor Wizard: Add Form

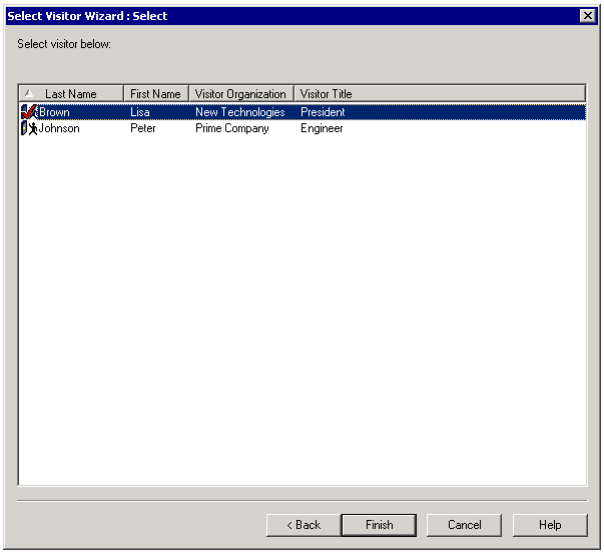
Form Element	Type	Comment
Last name	text	Indicates visitor's last name.
First name	text	Indicates visitor's first name.
Middle name	text	Indicates visitor's middle name.
Badge type	drop-down listbox	Select the visitor's badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.
User-defined fields		All fields below the Name fields on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.
Import	button	Displays the Select Import Source window, which allows you to select a device to import visitor data from, such as a business card scanner

Visits Folder - Select Visitor Wizard: Add Form (Continued)

Form Element	Type	Comment
Capture	button	Displays the Multimedia Capture Module, where you can capture photographic information such as a photo, signature or biometric data for a visitor
Back	push button	Returns to the Select Visitor Wizard: Select or Add form.
Finish	push button	Completes the wizard. The visitor record will be added to the database and the name of the visitor who was just added will be displayed in the **Visitor name** field.
Cancel	push button	Closes the window without adding a visitor and returns you to the Visit form in the Visits folder.
Help	push button	Displays online help for this topic

Select Visitor Wizard: Select Form

This form is displayed when the [...] button to the right of the Visitor name field on the Visit form in the Visits folder is clicked.



Select Visitor Wizard: Select Form Overview

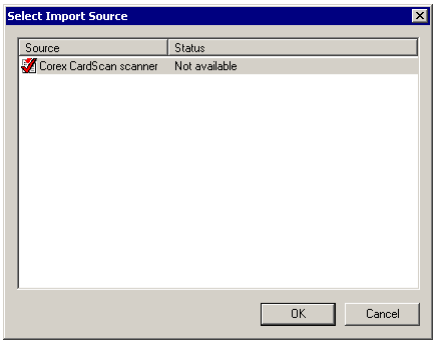
This form is displayed when searching; it is used to select a visitor record from those that matched the specified search criteria.

Visits Folder - Select Visitor Wizard: Select Form

Form Element	Type	Comment
Last Name	text	Indicates visitor's last name.
First Name	text	Indicates visitor's first name.
Middle Initial	text	Indicates visitor's middle initial.
User-defined fields		All fields below the Name fields on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.
Back	push button	Returns to the previous form.
Finish	push button	Completes the wizard. The selected visitor's name will be displayed in the **Visitor name** field.
Cancel	push button	Closes the window without selecting a visitor and returns you to the Visit form in the Visits folder.
Help	push button	Displays online help for this topic

Select Import Source Window

This window is displayed by clicking the [Import] button on any window in the Select Host Wizard or Select Visitor Wizard.



Select Import Source Window Field Table

Form Element	Type	Comment
Source listing window	display	Displays a list of available sources, such as a business card scanner, to import cardholder or visitor data from.
OK	push button	If a valid source is selected, you will be able to import cardholder or visitor data using it.
Cancel	push button	Closes the Select Import Source window without selecting a source to import cardholder or visitor data from.

Chapter 15: Reports Folder

The Reports folder contains forms with which you can:

- View on the screen reports created using report layout templates in the database and current data
- Report on data that meets specified criteria (such as dates, times, readers, alarm panels, cardholders and badge IDs)
- Print a report, save it to a file or export the data

The folder contains eight forms: the Report Configuration form, the Reader Reports form, the Alarm Panel Reports form, the Anti-Passback Reports form, the Date/Time Reports form, the Event Reports form, the Receiver Account Zone Reports form, and the Alarm Acknowledgment Reports form.

Toolbar Shortcut

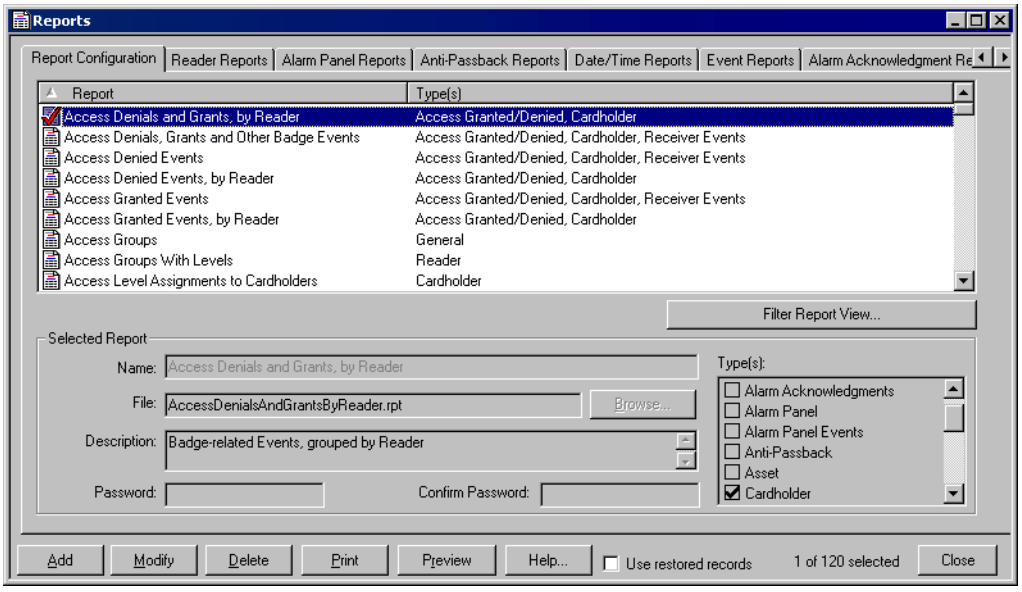
This folder is displayed by selecting **Reports** from the **View** menu or by selecting the Reports toolbar button.

Reports are installed when Database Setup is run. All reports are installed on the database server under the ReportTemplates subdirectory in the B.A.S.I.S. installation path. By default, this location is **C:\Program Files\B.A.S.I.S.\ReportTemplates**. For more information refer to The Database Setup Program appendix in the Installation & Setup User Guide.

Note: Refer to the release notes for the versions of Seagate Crystal Reports that are supported. The release notes are located on the root of the B.A.S.I.S. CD in a file named **B.A.S.I.S. ET release notes.rtf.**

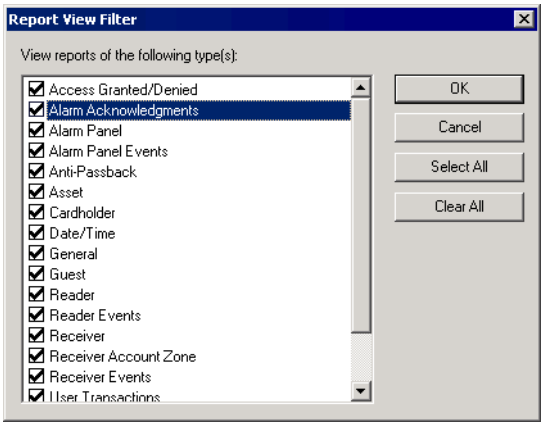
For more information, refer to Appendix C: Reports on page 415.

Report Configuration Form



Report View Filter Window

This window is displayed by clicking the [Filter Report View] button on the Report Configuration form.



Reports Folder - Report Configuration Form

Form Element	Type	Comment
Listing window	display	Lists currently defined reports of the type(s) selected in the Report View Filter window. Note that some reports are categorized under more than one type.

Reports Folder - Report Configuration Form (Continued)

Form Element	Type	Comment
Filter Report View	push button	Click this button to display the Report View Filter window from where you can choose the types of reports you wish to view.
Name	text	The name of the report.
File	text	The location and name of the file that contains the report.
Browse	push button	Used to search through drives and directories to choose a report filename to insert into the **File** field.
Description	text	A brief description of the report contents.
Password	text	This field is optional. If you type a password here, a user attempting to print this report will be asked to first enter the correct password. A password can be from 1 to 32 characters in length. As you type, the password will appear in the field as a series of *s.
Confirm Password	text	If you typed something in the **Password** field, you must type exactly the same thing here. As with the **Password** field, your entry here will appear as a series of *s.
Type(s)	section	Lists the types of reports that you can configure. The system reports that are included with the installation are each assigned an appropriate Type. You can modify report types on the system reports but selecting invalid types could result in unwanted behavior. **Note:** To restore types back to their defaults, run Database Setup. **Note:** To make the report appear in Area Access Manager the Area Access Manager checkbox must be selected in the Types field.
Add	push button	Used to configure a report.
Modify	push button	Used to change a report configuration.
Delete	push button	Used to remove a report.
Print	push button	Opens the Print Report Options window.
Preview	push button	Displays the selected report in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder.

Reports Folder - Report Configuration Form (Continued)

Form Element	Type	Comment
Mode	display	In view mode, indicates the number of reports selected in the listing window and the total number of reports contained in all selected categories. For example: “1 of 42 selected.” In modify mode, indicates the current operation, such as “Modify Mode.”
Close	push button	Closes the Reports folder.

Reports Folder - Report View Filter Window

Form Element	Type	Comment
Access Granted/ Denied	checkbox	If this checkbox is selected, Access Granted and Access Denied reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.
Alarm Acknowledgments	checkbox	If this checkbox is selected, Alarm Acknowledgment reports will be included in the listing window.
Alarm Panel	checkbox	If this checkbox is selected, Alarm Panel reports will be included in the listing window. Reports of this type appear on the Alarm Panel Reports form for filtering.
Alarm Panel Events	checkbox	If this checkbox is selected, Alarm Panel Events reports will be included in the listing window. Reports of this type appear on the Alarm Panel Reports form for filtering.
Anti-Passback	checkbox	If this checkbox is selected, Anti-Passback reports will be included in the listing window. Reports of this type appear on the Anti-Passback Reports form for filtering.
Asset	checkbox	If this checkbox is selected, Asset reports will be included in the listing window. Reports of this type appear on the Asset Reports form for filtering.
Cardholder	checkbox	If this checkbox is selected, Cardholder reports will be included in the listing window. Reports of this type appear on the Reports form of the Cardholder folder for filtering.
Date/Time	checkbox	If this checkbox is selected, Date/Time reports will be included in the listing window. Reports of this type appear on the Date/Time Report form for filtering.

Reports Folder - Report View Filter Window (Continued)

Form Element	Type	Comment
General	checkbox	If this checkbox is selected, general reports will be included in the listing window.
Guest	checkbox	If this checkbox is selected, guest reports will be included in the listing window.
Reader	checkbox	If this checkbox is selected, Reader reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.
Reader Events	checkbox	If this checkbox is selected, Reader Events reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.
Receiver	checkbox	If this checkbox is selected, the names of Receiver reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.
Receiver account Zone	checkbox	If this checkbox is selected, the names of Account Zone reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.
Receiver Events	checkbox	If this checkbox is selected, the names of Receiver Events reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.
User Transactions	checkbox	If this checkbox is selected, User Transactions reports will be included in the listing window. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder.
Video Events	checkbox	If this checkbox is selected, Video events reports will be included in the listing window.
Visitor	checkbox	If this checkbox is selected, Visitor reports will be included in the listing window.
OK	push button	Click this button to save your changes and return to the Report Configuration form.
Cancel	push button	Click this button to return to the Report Configuration form without saving your changes.
Select All	push button	Click this button to select all checkboxes in the window.
Clear All	push button	Click this button to deselect all checkboxes in the window.

Report Configuration Form Procedures

Add a Report

1. Select **Reports** from the **View** menu. The Reports folder opens.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the report.
4. Click [Browse]. The Open window opens.
5. Select the drive, then the directory, then the file name for an existing report layout.
6. Click [OK] to insert the selection into the **File** field on the Report Configuration form.

Note: You cannot use the Report Configuration form to design a report layout. Only existing layouts can be used to create reports. A valid report layout must have been designed using Crystal Reports for Windows™ and must have the file extension “rpt.”

---

7. In the **Description** field, type a description of this report's contents.
8. If you want to restrict previewing and printing of this report, type a password in the **Password** field.
9. Type the password again in the **Confirm Password** field.
10. In the **Type(s)** listing window, select the checkboxes beside the most appropriate category for this report.

Note: You do not have to select a checkbox. Many of the reports currently in the system are uncategorized.

---

11. Click [OK] to add the report. The name of the report will be inserted alphabetically into the listing window.

Modify a Report

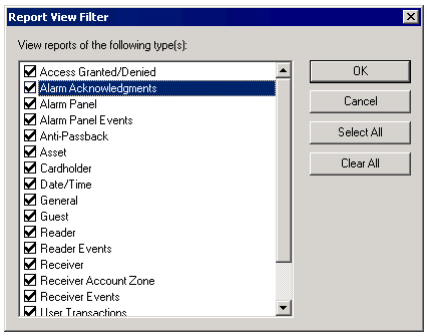
1. From the listing window, select the name of the report that you want to be changed. If the report is not listed, make sure that the appropriate checkbox is selected in the Report View Filter window (displayed by selecting the [Filter Report View] button).
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Report

1. From the listing window, select the name of the report that you want to delete. If the report is not listed, make sure that the appropriate checkbox is selected in the Report View Filter window (displayed by selecting the [Filter Report View] button).
2. Click [Delete].
3. Click [OK].

Filter The Report View

1. On the Report Configuration form, click [Filter Report View]. The Report View Filter window opens.

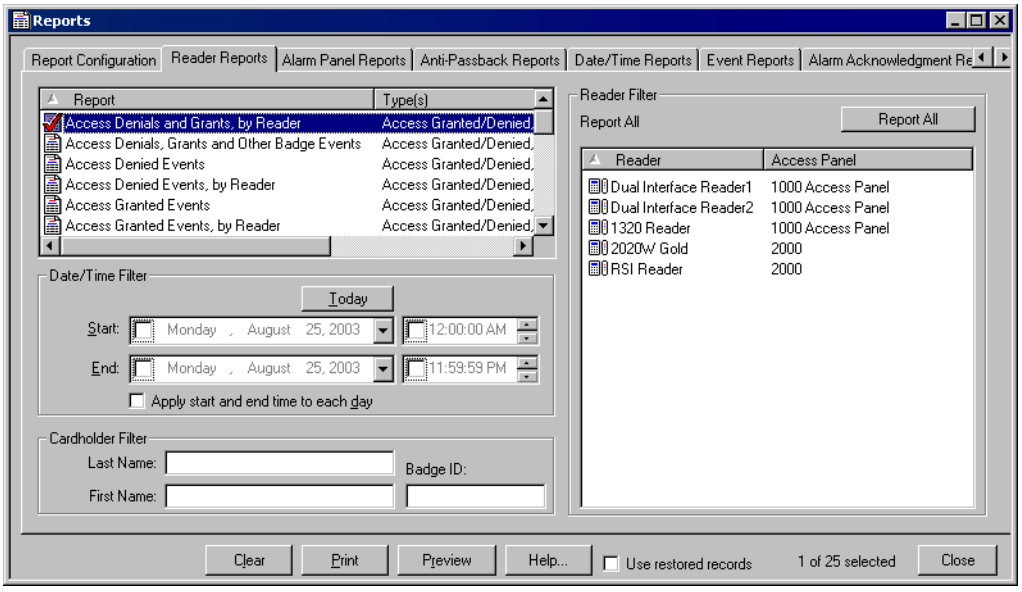


2. Select the checkboxes that correspond with the types of reports that you want to view. Click [Select All] to select all of the choices in the listing window. Click [Clear All] to deselect all of the choices in the listing window.
3. Click [OK]. The types of reports that correspond to the checkboxes that you selected will be displayed in the listing window on the Report Configuration form.

Preview and Print a Report

For more information, refer to Preview and Print a Report on page 306.

Reader Reports Form



Reader Reports Form Overview

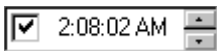
This form allows you to add filtering criteria to a reader report, so that you can narrow the results of your report. Depending on the type of report you select, you can optionally add a filter on reader(s), start date/time, end date/time, badge ID and/or cardholder name.

Reader Reports Form Field Table

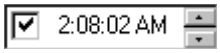
Readers Folder - Reader Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined reader reports, and each report's type. Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Readers Folder - Reader Reports Form (Continued)

Form Element	Type	Comment
Start con't	section	• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .

Readers Folder - Reader Reports Form (Continued)

Form Element	Type	Comment
End	section	• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Cardholder Filter	section	Includes the **Last Name**, **First Name**, and **Badge ID** fields. These fields are available only for applicable report types. These fields are not case-sensitive and will match any names beginning with the characters you type (much like the Cardholder form searches). For example, typing “smith” for Last Name will match “Smith”, “SMITHY”, “smithereen”, etc.
Last Name	text	Enter the cardholder’s last name.
First Name	text	Enter the cardholder’s first name.
Badge ID	numeric	If you wish to report on the activity associated with a specific badge, enter the Badge ID here. This field is available only for applicable report types.
Report All	push button	If this button is pushed, all entries in the **Reader** list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all readers will be included in the report.
Report All/__ selected	display	Indicates “Report All” if no devices are selected in the **Reader** field. Indicates “__ selected” if one or more devices are selected in the **Reader** field.

Readers Folder - Reader Reports Form (Continued)

Form Element	Type	Comment
Reader listing window	display	Lists all readers on the system and the access panel to which each is attached. To select/deselect a reader, click on the icon beside it. A "ü" on an icon indicates that the reader is selected. Only data from selected readers will be included in the report. However, if no devices are selected, data for all readers will be reported.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current "live" events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder in the System Administration User Guide.
Close	push button	Closes the Reports folder.

Reader Reports Form Procedures

Run a Reader Report

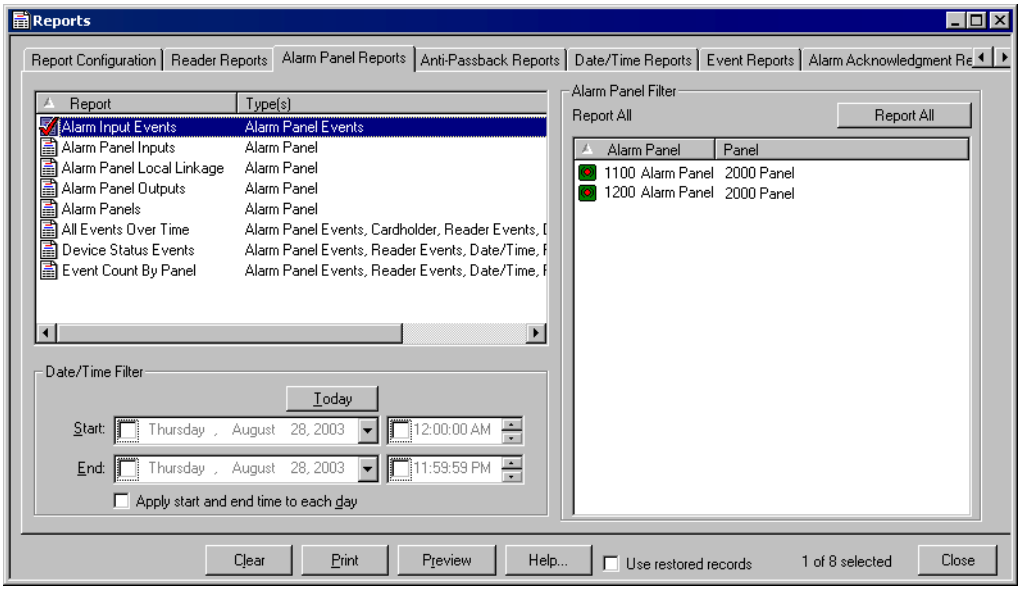
1. Select **Reports** from Administration **View** menu. The Reports folder opens.
2. Select the Reader Reports tab.
3. From the listing window, select the report that you want to run.
4. In the **Reader Filter** section, select the icon(s) corresponding to the reader(s) whose data you wish to include in the report. If you don't select any readers, data for all readers will be reported.
5. If desired, specify a date/time interval for gathering data in the **Date/Time Filter** section. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.
6. In the **Cardholder Filter** section, enter the person's **Last Name**, **First Name,** and/or **Badge ID** if you want the report to contain data pertaining

only to cardholders having the specified name and/or badge ID (cardholder name and badge ID is applicable only to reader reports based on events).

7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Alarm Panel Reports Form

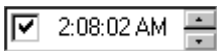


Alarm Panel Reports Form Overview

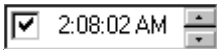
This form allows you to add filtering criteria to an alarm panel report, so that you can narrow the results of your report. Depending on the type of report you select, you can optionally add a filter on alarm panel(s), start date/time, and end date/time.

Alarm Panel Reports Form Field Table

Reports Folder - Alarm Panel Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined alarm panel reports, and each report's type. Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year and use the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.
		• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Alarm Panel Reports Form (Continued)

Form Element	Type	Comment
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the last year for which data is to be included in this report. To change the year, click on the name of the year to access the spin buttons .
		• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Alarm Panel Reports Form (Continued)

Form Element	Type	Comment
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Report All	push button	If this button is pushed, all entries in the **Alarm Panel** list are deselected. "Report All" is displayed to the left of this button, to indicate that data for all readers will be included in the report.
Report All /__ selected	display	Indicates "Report All" if no devices are selected in the **Alarm Panel** field. Indicates "__ selected" if one or more devices are selected in the **Alarm Panel** field.
Alarm Panel listing window	display	Lists all alarm panels on the system and the access panel to which each is attached. To select/deselect an alarm panel, click on the icon beside it. A "ü" on an icon indicates that the alarm panel is selected. Only data from selected alarm panels will be included in the report. However, if no devices are selected, data for all alarm panels will be reported.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current "live" events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder chapter in the System Administration User Guide.
Close	push button	Closes the Reports folder.

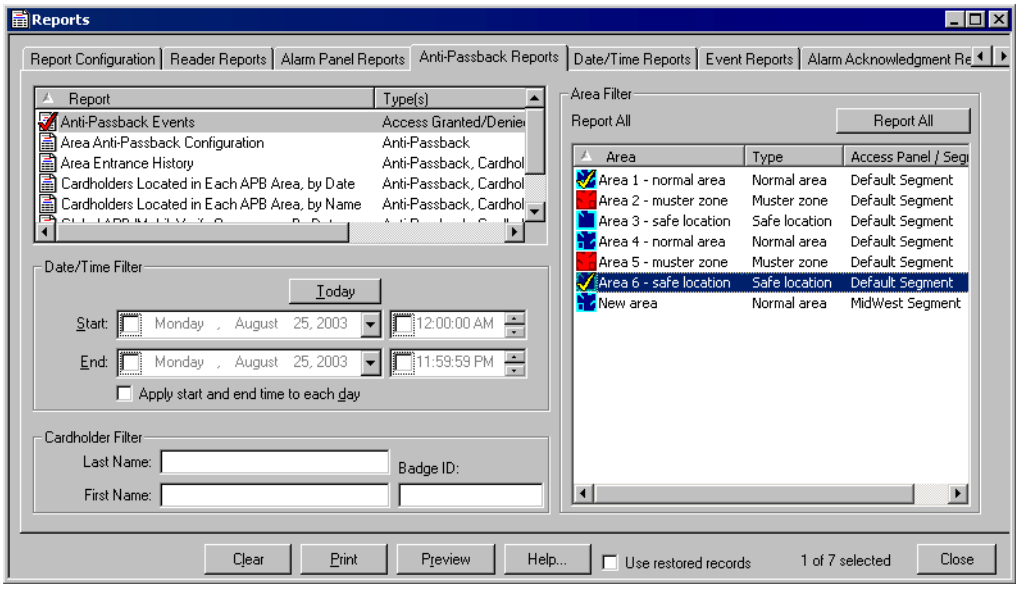
Alarm Panel Reports Form Procedures

Run an Alarm Panel Report

1. Select **Reports** from Administration **View** menu. The Reports folder opens.
2. Select the Alarm Panel Reports tab.
3. From the listing window, select the report that you want to run.
4. If desired, specify a date/time interval for gathering data in the **Date/Time Filter** section. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.
5. In the **Alarm Panel Filter** section, select the icon(s) corresponding to the alarm panel(s) whose data you wish to include in the report. If you don't select any alarm panels, or click [Report All], data for all alarm panels will be reported.
6. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Anti-Passback Reports Form

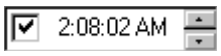


Anti-Passback Reports Form Overview

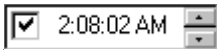
This form allows you to add filtering criteria to an anti-passback report, so that you can narrow the results of your report. Depending on the type of report you select, you can optionally add a filter on area(s), start date/time, end date/time, badge ID and/or cardholder name.

Anti-Passback Reports Form Field Table

Reports Folder - Anti-Passback Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined anti-passback reports, and each report(s) type. Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.
		• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Anti-Passback Reports Form (Continued)

Form Element	Type	Comment
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Anti-Passback Reports Form (Continued)

Form Element	Type	Comment
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Cardholder Filter	section	Includes the **Last Name**, **First Name**, and **Badge ID** fields. These fields are available only for applicable report types. These fields are not case-sensitive and will match any names beginning with the characters you type (much like the Cardholder form searches). For example, typing “smith” for Last Name will match “Smith”, “SMITHY”, “smithereen”, etc.
Last Name	text	Enter the cardholder’s last name.
First Name	text	Enter the cardholder’s first name.
Badge ID	numeric	If you wish to report on the activity associated with a specific badge, enter the Badge ID here. This field is available only for applicable report types.
Report All	push button	If this button is pushed, all entries in the **Area** list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all areas will be included in the report.
Report All /__ selected	display	Indicates “Report All” if no entries are selected in the **Area** field. Indicates “__ selected” if one or more entries are selected in the **Area** field.
Area listing window	display	Lists all anti-passback areas defined on the system, and the access panel associated with each. To select/deselect an area, click on the icon beside it. A “□” on an icon indicates that the area is selected. Only data pertaining to selected areas will be included in the report. However, if no entries are selected, data for all areas will be reported.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.

Reports Folder - Anti-Passback Reports Form (Continued)

Form Element	Type	Comment
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current "live" events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder chapter in the System Administration User Guide.
Close	push button	Closes the Reports folder.

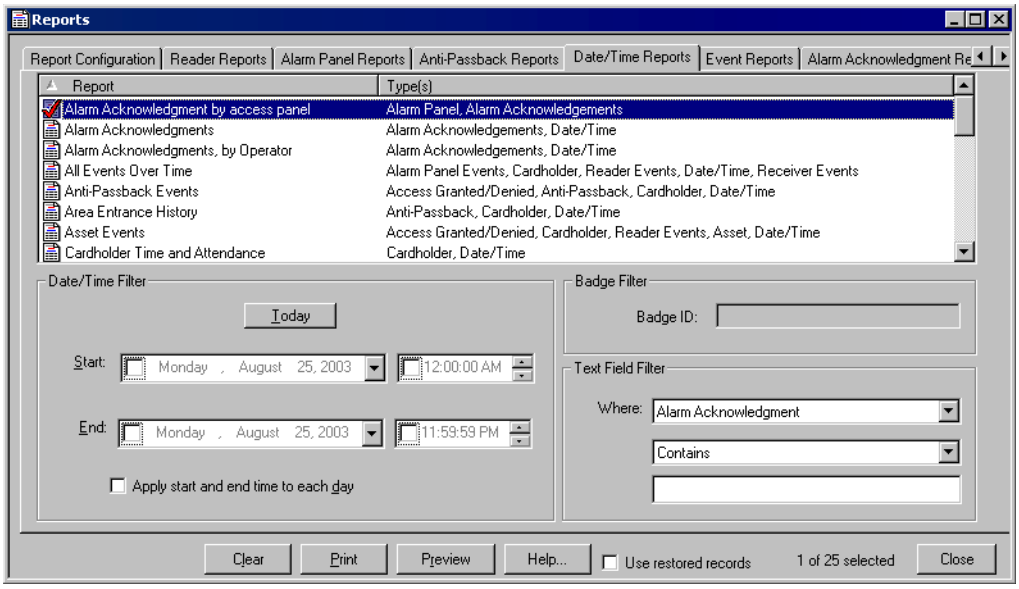
Anti-Passback Reports Form Procedures

Run an Anti-Passback Report

1. Select **Reports** from Administration **View** menu. The Reports folder opens.
2. Select the Anti-Passback Reports tab.
3. In the reports listing window, select the icon that corresponds to the report you wish to run.
4. Complete the **Date/Time Filter** section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.
5. In the **Cardholder Filter** section, enter the person's **Last Name**, **First Name**, and/or **Badge ID** if you want the report to contain data pertaining only to cardholders having the specified name or badge ID.
6. In the **Area Filter** section, select the icon(s) corresponding to the anti-passback area(s) whose data you wish to include in the report. If you don't select any areas, or click [Report All], data for all areas will be reported.
7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Date/Time Reports Form

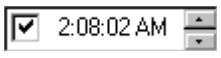


Date/Time Reports Form Overview

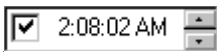
This form allows you to add filtering criteria to a date/time report, so that you can narrow the results of your report.

Date/Time Reports Form Field Table

Reports Folder - Date/Time Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined date/time reports, and each report(s) type. Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.
		• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Date/Time Reports Form (Continued)

Form Element	Type	Comment
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Date/Time Reports Form (Continued)

Form Element	Type	Comment
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Badge ID	numeric	If you wish to report on the activity associated with a specific badge, enter the Badge ID here. This field is available only for applicable report types.
Text Field Filter	section	Includes the **Where** and **Match criteria** fields, as well as a **Blank field**. This section is enabled only when a report that allows filtering is selected in the listing window.
Where	drop-down list	You can now add a text filter to the following: • Action Type, Details, or Object for User Transactions reports • Alarm Acknowledgment text for Alarm Acknowledgments reports When this section is enabled, the **Where** field contains the attribute in B.A.S.I.S. that is to be filtered.
Match criteria (Set to Contains by default. May also be set to Begins With, Ends With, or Equals)	drop-down list	If enabled, the **Match criteria** drop-down list may be changed from its default value of contains to Begins With, Ends With, or Equals. This setting specifies how the selection in the **Where** field relates to the value entered to search for in the **Blank field**.
Blank field	text	In this field, type the value you wish to filter or search for. For example, if you wanted to display all User Transactions associated with System Administration, you should: 1. Select a User Transaction Log report in the listing window. 2. In the **Where** field, select “Object”. 3. In the **Match criteria** field, select “Equals”. 4. In the blank field, type “System Administration” (without the quotes). Click [Preview], and only those entries associated with System Administration will be displayed in the resulting report.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.

Reports Folder - Date/Time Reports Form (Continued)

Form Element	Type	Comment
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder chapter in the System Administration User Guide.
Close	push button	Closes the Reports folder.

Date/Time Reports Form Procedures

Run a Date/Time Report

1. Select **Reports** from Administration **View** menu. The Reports folder opens.
2. Select the Date/Time Reports tab.
3. In the reports listing window, select the icon that corresponds to the report you wish to run.
4. Complete the **Date/Time Filter** section to specify a date/time interval for gathering data. Only data gathered during the specified period will be

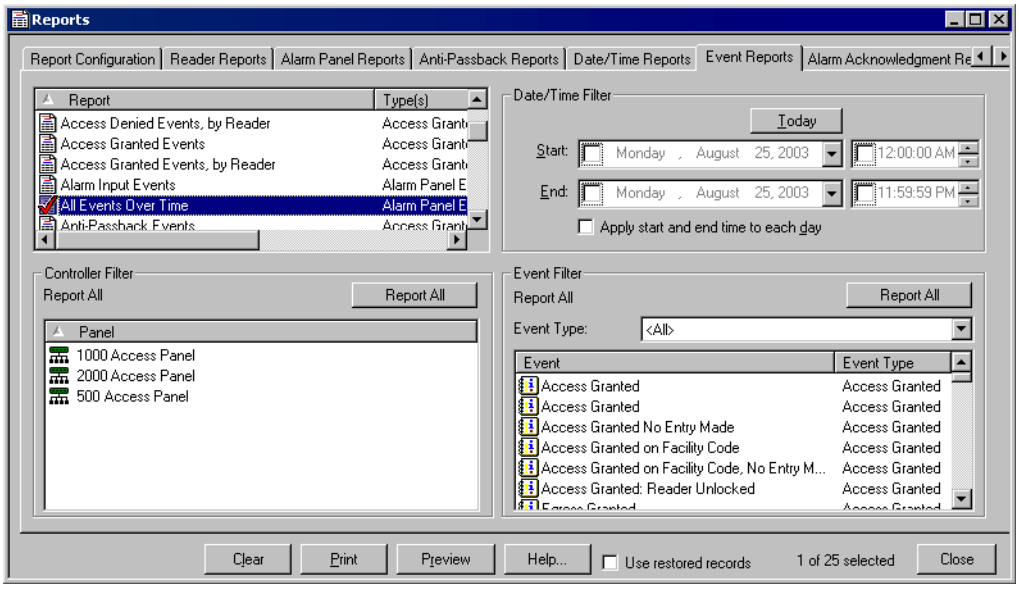
included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.

5. Enter a **Badge ID** if you want the report to contain data pertaining only to cardholders having the specified name or badge ID.
6. Complete the **Text Field Filter** section. (This section is optional, and is only enabled for User Transactions reports and Alarm Acknowledgment reports.)
   a. Select a value to filter in the **Where** field.
      - If the report you are running is a User Transactions report and you wish to apply a filter, select Action Type, Details, or Object in the **Where** field.
      - If the report you are running is an Alarm Acknowledgment report and you wish to apply a filter, select Alarm Acknowledgment in the **Where** field.

   b. In the next drop-down list, select whether the filter criteria **Begins With**, **Contains**, **Ends With** or **Equals** the value that you will enter in the next blank field.
   c. In the blank field, type the value you wish to filter for.
7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that's currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Event Reports Form



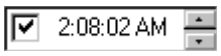
Note: On the Event Reports form, any report in the reports listing window that has "Cardholder" listed in the **Type(s)** column is available on the Reports form in the Cardholders folder. This means that a report can be generated on the Reports form in the Cardholders folder based on a cardholder search operation.

Event Reports Form Overview

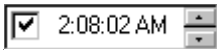
This form allows you to add filtering criteria to an event report, so that you can narrow the results of your report.

Event Reports Form Field Table

Reports Folder - Event Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined event reports, and each report's type(s). Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.
		• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Event Reports Form (Continued)

Form Element	Type	Comment
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the last year for which data is to be included in this report. To change the year, click on the name of the year and use the spin buttons .
		• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.

Reports Folder - Event Reports Form (Continued)

Form Element	Type	Comment
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Report All (panels)	push button	If this button is pushed, all entries in the **Panel** list are deselected. "Report All" is displayed to the left of this button, to indicate that data for all access panels will be included in the report.
Report All / __ selected	display	Indicates "Report All" if no entries are selected in the **Panel** field. Indicates "__ selected" if at least one entry is selected in the **Panel** field.
Panel listing window	display	Lists all panels in the system. An icon that indicates the panel's type precedes each entry. If your installation uses segmentation, the segment assignment is listed for each entry.
Report All (events)	push button	If this button is pushed, all entries in the **Event** list are deselected. "Report All" is displayed to the left of this button, to indicate that data for all events for the selected **Event Type** will be included in the report.
Report All / __ selected	display	Indicates "Report All" if no entries are selected in the **Event** field. Indicates "__ selected" if at least one entry is selected in the **Event** field.
Event Type	drop-down list	Can be used to filter all events of a particular type. For example, if you select the "All Events Over Time" report and select an **Event Type** of "Fire", an "All Fire Events Over Time" report will effectively be created.
Event listing window	display/listing window	Lists currently defined events for the selected **Event Type**, and each event's type.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.

Reports Folder - Event Reports Form (Continued)

Form Element	Type	Comment
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder chapter in the System Administration User Guide.
Close	push button	Closes the Reports folder.

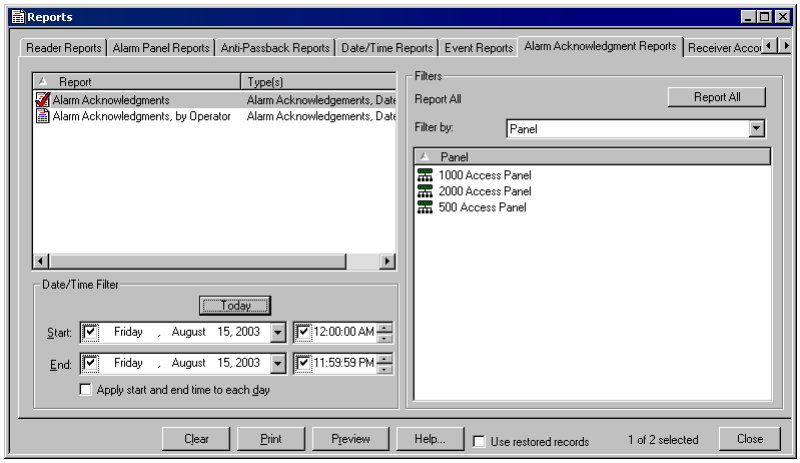
Event Reports Form Procedures

Run an Event Report

1. Select **Reports** from the **View** menu. The Reports folder opens.
2. Select the Event Reports tab.
3. In the reports listing window, select the icon that corresponds to the report you wish to run.
4. Complete the **Date/Time Filter** section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.
5. In the **Access Panel Filter** section, select the icon(s) corresponding to the panel(s) whose data you wish to include in the report. If you don’t select any panels, or click [Report All], data for all panels will be reported.
6. In the **Event Filter** section, select an **Event Type**.
7. In the **Event** listing window, select the icon(s) corresponding to the event(s) whose data you wish to include in the report.
   - If you select “<All>” in the **Event Type** field, data for all events will be reported.
   - If you click [Report All], data for all events of the selected **Event Type** will be reported.
8. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that’s currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Alarm Acknowledgment Reports Form



Alarm Acknowledgment Reports Form Overview

The Alarm Acknowledgment Reports form is designed to provide reports on acknowledged alarms. This report can be filtered by the date/time the acknowledgment occurred, the device that triggered the alarm, and the operator who acknowledged the alarm. When you select a filter, the report displays alarm acknowledgments for only the filtered device. If you want to view everything, use the convenient [Report All] button.

The result of the report includes the following:

- Date and time this report was created
- Date and time the alarm occurred
- Date and time the alarm was acknowledged
- Who acknowledged the alarm
- Any notes included with the acknowledgment
- The device that caused the alarm
- The total number of acknowledgments

Notes: The details column does not report who acknowledged the alarm, but rather who was logged into Alarm Monitoring when the alarm was acknowledged. Therefore, someone other than the person logged into Alarm Monitoring may have acknowledged the alarm.

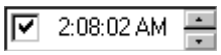
The first and last name displayed in the Details column are configured in the System Administration Users folder.

Alarm Acknowledgment Reports Form Field Table

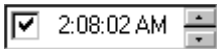
Reports Folder - Alarm Acknowledgment Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined alarm acknowledgment reports, and each report's type(s). Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year to access the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Reports Folder - Alarm Acknowledgment Reports Form (Continued)

Form Element	Type	Comment
Start	section	• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the last year for which data is to be included in this report. To change the year, click on the name of the year to access the spin buttons .

Reports Folder - Alarm Acknowledgment Reports Form (Continued)

Form Element	Type	Comment
End	section	• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Report All	push button	Reports every alarm acknowledgment and does not apply any filter.
Filter by	drop-down list	Select one device you want the report based on. The report displays the alarm acknowledgments only for the device you select.
Filter listing window	display	Select one or multiple filters for the report. The filters that display in this window depend on what you select in the **Filter by** drop-down list. The report displays the alarm acknowledgments for only the devices you select.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.

Reports Folder - Alarm Acknowledgment Reports Form (Continued)

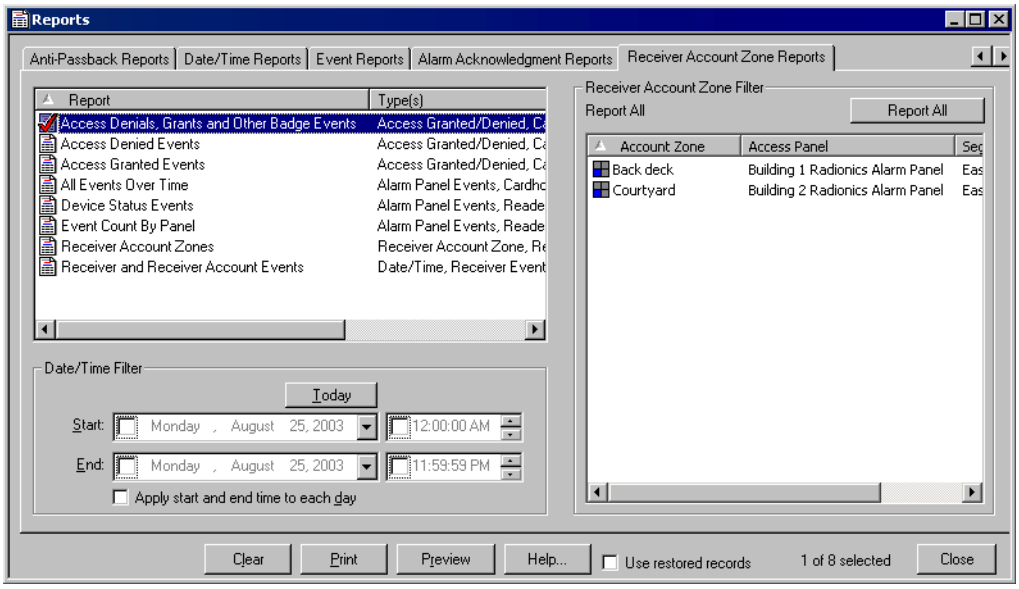
Form Element	Type	Comment
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder chapter in the System Administration User Guide.
Close	push button	Closes the Reports folder.

Run an Alarm Acknowledgment Report

1. Select **Reports** from the **View** menu. The Reports folder opens.
2. Select the Alarm Acknowledgment Reports tab.
3. In the listing window, select the report you wish to run.
4. Complete the **Date/Time Filter** section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.
5. In the **Filter by** drop-down list, select the device whose data you wish to include in the report. If you don’t select any device, or if you click [Report All], data for every device will be reported.
6. In the Filter listing window, select the device(s) whose data you wish to include in the report.
7. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that’s currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

Receiver Account Zone Reports Form



Receiver Account Zone Reports Form Overview

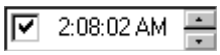
This form allows you to add filtering criteria to a receiver account zone report, so that you can narrow the results of your report.

Receiver Account Zone Reports Form Field Table

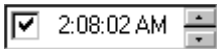
Reports Folder - Receiver Account Zone Reports Form

Form Element	Type	Comment
Listing window	display	Lists currently defined alarm acknowledgment reports, and each report's type(s). Note that some reports are categorized under more than one type.
Today	push button	Click this button to: • Set the Start time/date to 12:00:00 AM on the current date • Set the End time/date to 11:59:59 PM on the current date
Start	section	If you want to filter a report by a specific date, select the **Start date** checkbox and choose a specific start date from the drop-down calendar.
		• Select the first month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year to access the spin buttons .
		• Once you have selected a month and a year, click on the first day for which data is to be included in this report. Note that the day circled in red indicates the current date.

Reports Folder - Receiver Account Zone Reports Form (Continued)

Form Element	Type	Comment
Start	section	• Select the time for which data is to be included in this report by selecting the **Start time** checkbox and choosing a specific start time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.
End	section	If you want to filter a report by a specific date, select the **End date** checkbox and choose a specific end date from the drop-down calendar.
		• Select the last month for which data is to be included in this report. Use the and navigation buttons to view different months. You can also click on the name of the month to access a drop-down list of every month.
		• Select the first year for which data is to be included in this report. To change the year, click on the name of the displayed year to access the spin buttons .

Reports Folder - Receiver Account Zone Reports Form (Continued)

Form Element	Type	Comment
End	section	• Once you have selected a month and a year, click on the last day for which data is to be included in this report. Note that the day circled in red indicates the current date. • Select the time for which data is to be included in this report by selecting the **End time** checkbox and choosing a specific end time.  Highlight the hour, minutes, or seconds by clicking on them. Use the spin buttons to increase or decrease their value. To change from AM to PM, highlight AM by clicking on it, and use the spin buttons.
Apply start and end time to each day	checkbox	If selected, the specified time range will be applied to any date that falls within the specified date range. For example, if you specify a Date/Time Filter starting January 1, 1998 at 8:00 AM and ending March 31, 1998 at 7:00 PM: • If this box is checked, the report will include only data collected during the hours of 8:00 AM through 7:00 PM, on any and all days between January 1 and March 31. • If this box is not checked, the report will include all data gathered from 8:00 AM on January 1 straight through until March 31 at 7:00 PM.
Report All (account zones)	push button	If this button is pushed, all entries in the **Account Zone** list are deselected. “Report All” is displayed to the left of this button, to indicate that data for all account zones will be included in the report.
Report All/___ selected	display	Indicates “Report All” if no entries are selected in the **Account Zone** field. Indicates “__ selected” if at least one entry is selected in the **Account Zone** field.
Account Zone listing window	display	Lists all account zones in the system. An icon that indicates the account zone’s type precedes each entry. If your installation uses segmentation, the segment assignment is listed for each entry.
Clear	push button	Clears all current filter criteria.
Print	push button	Displays the Print Report Options window.
Preview	push button	Displays the selected report with selected criteria in the Report Print Preview window.
Help	push button	Displays relevant on-screen help for this form.

Reports Folder - Receiver Account Zone Reports Form (Continued)

Form Element	Type	Comment
Use restored records	checkbox	If this checkbox is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder. For more information refer to the Archives Folder chapter in the System Administration User Guide.
Close	push button	Closes the Reports folder.

Receiver Account Zone Reports Form Procedures

Run a Receiver Account Zone Report

1. Select **Reports** from the **View** menu. The Reports folder opens.
2. Select the Receiver Account Zone Reports tab.
3. In the listing window, select the icon that corresponds to the report you wish to run.
4. Complete the **Date/Time Filter** section to specify a date/time interval for gathering data. Only data gathered during the specified period will be included in the report. To limit each date in the range to the specified time interval, select the **Apply start and end time to each day** checkbox.
5. In the **Account Zone Filter** section, select the icon(s) corresponding to the account zone(s) whose data you wish to include in the report. If you don’t select any account zones, or if you click [Report All], data for all account zones will be reported.
6. Click either the [Print] or [Preview] button depending on which function you wish to perform. For more information, refer to Chapter 18: Report Print Preview Window on page 303.

Note: Only data that’s currently in the database can be included in the report. Events or other transactions deleted because of space limitations or elapsed time are no longer available.

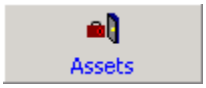
Chapter 16: Assets Folder

The Assets folder contains forms with which you can:

- Add, change or remove asset records.
- Assign assets to cardholders.
- Track assets that are assigned to cardholders.
- Preview and print asset reports.

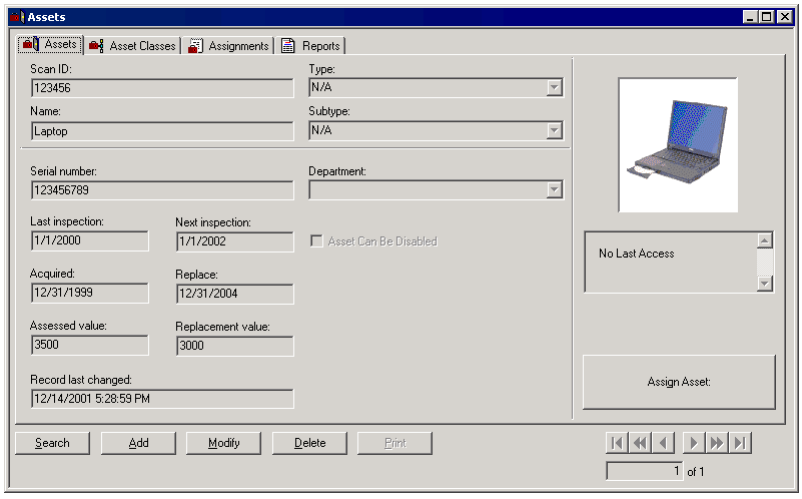
The Assets folder contains four forms: the Assets form, the Asset Classes form, the Assignments form and the Reports form.

Toolbar Shortcut



This folder is displayed by selecting the **Asset Info** from the **View** menu.

Assets Form



Assets Folder - Assets Form

Form Element	Type	Comment
Scan ID	numeric	Enter the Scan ID of the asset.
Name	text	Enter a descriptive name for the asset. This is a “friendly” name assigned to each asset to make it easy to identify. Each name must be unique and contain no more than 32 characters.
Type	drop-down list	Select the type of asset being configured. Available choices depend on what asset types were added in the Asset Types and Subtypes Management window. The window is displayed by selecting **Asset Types and Subtypes** from the **Asset** menu.
Subtype	drop-down list	Select the subtype of the asset being configured. Available choices depend on what asset subtypes were added in the Asset Types and Subtypes Management window. The window is displayed by selecting **Asset Types and Subtypes** from the **Asset** menu.
Serial Number	numeric	Enter the serial number of the asset you are adding.
Department	drop-down list	Select the department of the asset being configured. Available choices depend on what departments were added in the List Builder folder.
Last Inspection	numeric	Enter the date when the asset was last inspected.
Next Inspection	numeric	Enter the date when the asset will be inspected next.
Acquired	numeric	Enter the date when the asset was acquired.
Replace	numeric	Enter the date when the asset will be replaced.
Assessed Value	numeric	Enter the assessed value of the asset.
Replacement Value	numeric	Enter the replacement value of the asset.

Assets Folder - Assets Form (Continued)

Form Element	Type	Comment
Asset Can Be Disabled	checkbox	(For special HID, IBM notebooks only) If checked, when the asset generates an access denied alarm (when a cardholder is not assigned to the asset), the asset will be disabled. The **Can Disable Asset** checkbox on the Settings form of the Readers folder in System Administration must also be checked in order for the selected reader to disable the asset.
Record Last Changed	display	Indicates the date of when the selected asset record was last changed.
Photo	display	Displays a photo capture of the asset if one was added in the Multimedia Capture module.
Last Access	display	Displays the date and time of the asset's last access.
Assign Asset/ Assign To	push button	When adding or modifying an asset, select the [Assign Asset] button to launch the Cardholders folder. On the Cardholder form you can search for or add a cardholder to assign to the asset being configured. Once you have located the cardholder on the Cardholder form, their name will appear on the [Assign To] push button. Click on this button to assign the asset to the cardholder. If the Cardholders folder is already open and a cardholder record is displayed, then the [Assign To] button will automatically display the name of that cardholder record.
Search	push button	Click on this button to search for an asset based on a value entered in one or more of the fields.
Last Search	push button	Click on this button the display the findings of the previous search.
	push button	Moves to the first matching record.
	push button	Moves 10 matching records back.
	push button	Moves to the previous matching record.
	push button	Moves to the next matching record.
	push button	Moves 10 matching records forward.
	push button	Moves to the last matching record.
Record count	numeric	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.

Assets Folder - Assets Form (Continued)

Form Element	Type	Comment
Add	push button	Used to add an asset record.
Capture	push button	Launches the Multimedia Capture module where you can add a photo of the asset.
Modify	push button	Used to change an asset record.
Delete	push button	Used to delete an asset record.
Print	push button	This button is not used.

Assets Form Procedures

Add an Asset

Note: This procedure does not apply to view/edit only workstations.

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Click [Add].
3. In the **Scan ID** field, enter an ID number for the asset.
4. In the **Name** field, enter a descriptive name for the asset. This is a "friendly" name assigned to each asset to make it easy to identify. Each name must be unique and contain no more than 32 characters.
5. If you want to identify the asset by type, select one from the **Type** drop-down list. If you want to identify the asset by subtype, select one from the **Subtype** drop-down list. If you don't want to identify the asset by type and/or subtype, choose N/A from the **Type** and **Subtype** drop-down lists.
6. Type in a **Serial Number** and then choose the **Department** of the asset from the drop-down list.
7. Enter the date of the asset's **Last Inspection** and the date of the asset's **Next Inspection**.
8. Enter the date of when the asset was acquired in the **Acquired** field.
9. Enter the date of when the asset will be replaced in the **Replace** field.
10. In the **Assessed Value** field type the amount, in dollars, of the asset's value. In the **Replacement Value** field type the amount, in dollars, it will cost to replace the asset.
11. Check the **Asset Can Be Disabled** checkbox if the asset can and you want it to be disabled when the asset generates an access denied alarm (when a cardholder is not assigned to the asset.) The **Can Disable Asset** checkbox on the Settings form of the Readers folder in the System Administration

application must also be checked in order for the selected reader to disable the asset.

12. Click [Capture] to launch the Multimedia Capture module from where you can capture a photo of the asset to be displayed on the Assets form. For more information refer to the Multimedia Capture Module appendix in the System Administration User Guide.
13. You can switch to the Asset Classes form if you want to configure groups and classes now. For more information, refer to Asset Classes Form Procedures on page 288.
14. Click [OK].

Modify an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the asset record that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

Delete an Asset

Note: This procedure does not apply to view/edit only workstations.

1. Locate the asset record that you want to delete.
2. Click [Delete].
3. Click [OK].

Assign a Cardholder to an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the asset record that you want to assign.
2. If the Cardholders folder was already open and a cardholder record displayed, proceed to 3. If not, click [Assign Asset] to launch the Cardholders folder.
3. In the Cardholders folder, retrieve the record of the cardholder you want to assign to the asset. On the Assets form of the Assets folder, the name of the cardholder will appear in the [Assign To] push button.
4. Click [Assign To] to assign the asset.

Search for an Asset Record

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Click [Search].
3. Specify your search criteria by typing full partial entries in the enabled fields.
4. Click [OK].

   B.A.S.I.S. retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Retrieve the Most Recent Search Results

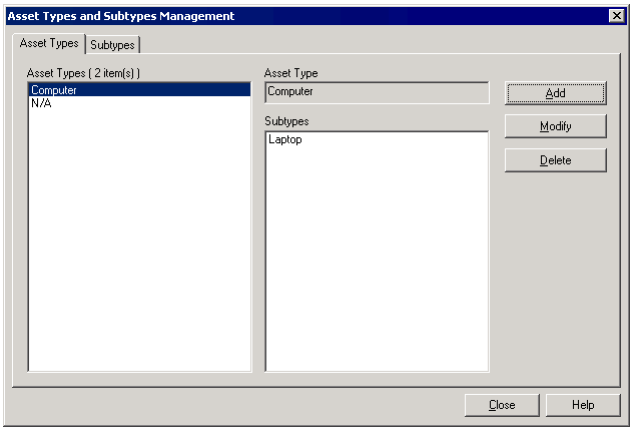
1. Click [Search].
2. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
3. If you want, modify your search criteria.
4. Click [OK].

   B.A.S.I.S. retrieves and displays the first matching record. Use the , , , , and buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Add an Asset Type/Subtype

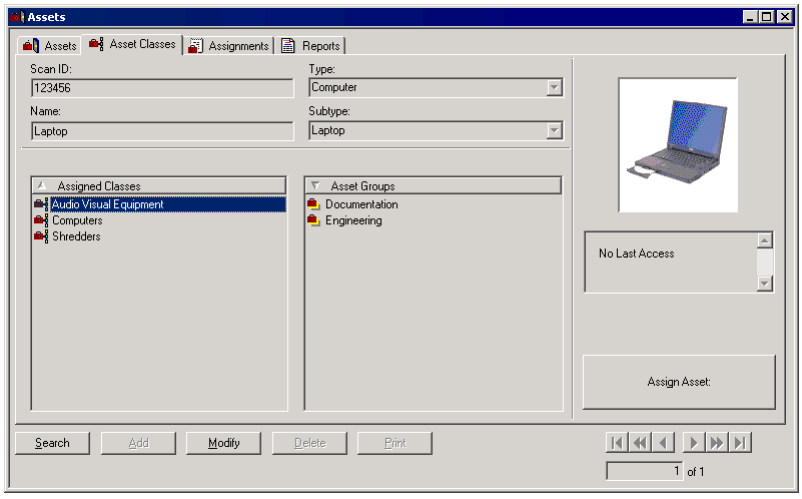
Note: This procedure does not apply to view only workstations.

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Select **Asset Types and Subtypes** from the **Asset** menu. The **Asset Types and Subtypes Management** window opens.

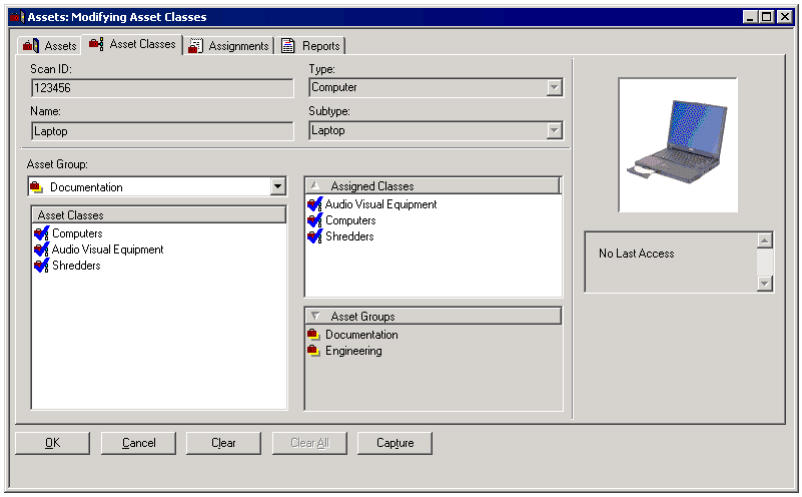


3. Click [Add].
4. Enter the name of the asset type.
5. Do one of the following:
   - If you don't want to add subtypes to this asset type, click [OK].
   - If you want to add a subtype, select the Subtype tab then click [Add]. Enter the name of the subtype, then click [OK].
6. Click [Close] to return to the Assets form.

Asset Classes Form (View Mode)



Asset Classes Form (Modify Mode)



Asset Classes Form Field Table

Assets Folder - Asset Classes Form

Form Element	Type	Comment
Scan ID	numeric	Indicates the Scan ID of the asset.
Name	text	Indicates the name of the asset.
Type	drop-down list	Indicates the type of asset being configured.
Subtype	drop-down list	Indicates the subtype of the asset being configured.
Assigned Classes	listing window	(View and modify mode) Displays the classes that are currently assigned to a group in the Asset Groups listing window.
Asset Groups	listing window	(View mode) Displays the asset groups that correspond with the classes in the Assigned Classes listing window.
Asset Group	drop-down list	(Modify mode) Select the asset group(s) to which the asset will belong.
Asset Classes	listing window	Select the asset classes that will be assigned to the asset. Groups can contain as many as 32 classes, but each asset can only belong to as many as 15 classes.
Photo	display	Displays a photo capture of the asset if one was added in the Multimedia Capture module.
Last Access	display	Displays the date and time of the asset's last access.
Assign Asset/ Assign To	push button	When adding or modifying an asset, select the [Assign Asset] button to launch the Cardholders folder. On the Cardholders form you can search for or add a cardholder to assign to the asset being configured. Once you have located the cardholder on the Cardholders form, their name will appear on the [Assign To] push button. Click on this button to assign the asset to the cardholder. If the Cardholders folder is already open and a cardholder record is displayed, then the [Assign To] button will automatically display the name of that cardholder record.
Search	push button	Click on this button to search for an asset based on a value entered in one or more of the fields.
Last Search	push button	Click on this button the display the findings of the previous search.
	push button	Moves to the first matching record.
[	push button	Moves 10 matching records back.
	push button	Moves to the previous matching record.
	push button	Moves to the next matching record.
	push button	Moves 10 matching records forward.

Assets Folder - Asset Classes Form (Continued)

Form Element	Type	Comment
	push button	Moves to the last matching record.
Record count	numeric	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Add	push button	This button is not used.
Modify	push button	Used to change an asset classes record.
Delete	push button	This button is not used.
Print	push button	This button is not used.

Asset Classes Form Procedures

Assign Classes to an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the record of the asset that you want to assign classes to.
2. Click Modify].
3. Select an **Asset Group** from the drop-down list.
4. In the **Asset Classes** listing window, select the classes you want to assign. You can select as many as 15 classes for each asset.
5. Click [OK].

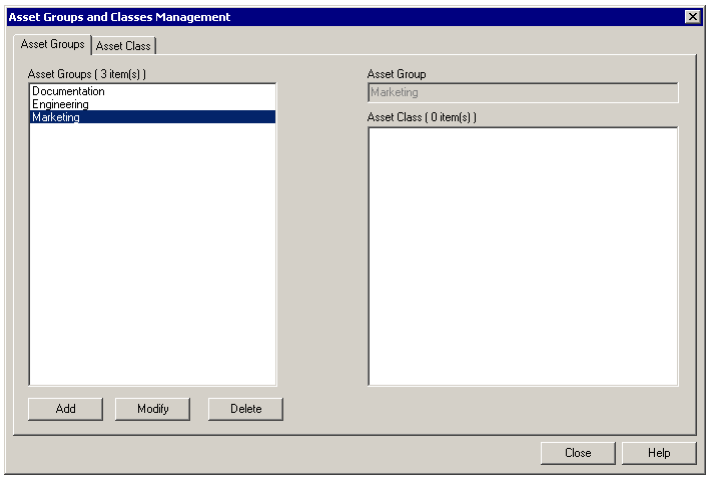
Modify an Asset Classes Assignment

Note: This procedure does not apply to view only workstations.

1. Locate the record of the asset that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

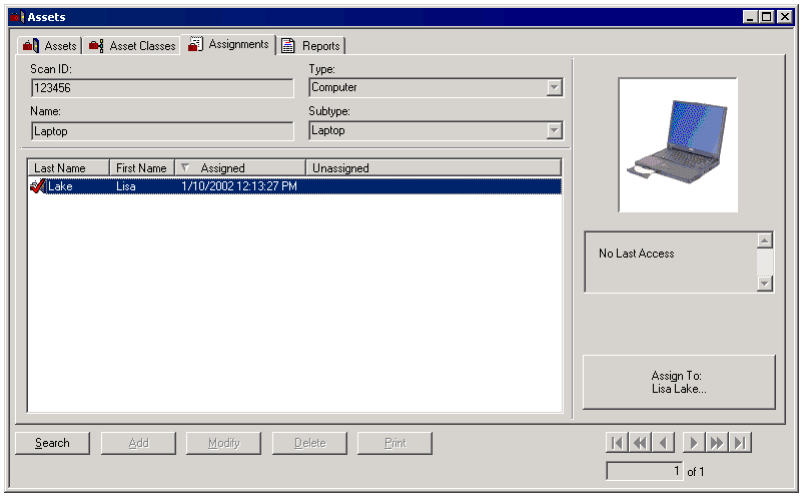
Add Asset Groups and Classes

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Select **Asset Groups and Classes** from the **Asset** menu. The **Asset Groups and Classes Management** window opens.



3. To add an asset group, click [Add].
4. In the **Asset Group** field, enter the name of the group you are adding.
5. Click [OK].
6. To add an asset class, select the Asset Class tab, then click [Add].
7. In the **Asset Class** field, enter the name of the class you are adding. You can add as many classes as you want but you can only assign as many as 32 classes to a group.
8. To assign a class to a group, select the name of a group in the **Asset Groups** listing window.
9. Click [Modify].
10. Select the name of the class you want to add in the **Asset Class** listing window.
11. Click the <-- push button. To remove the asset from the group, select the class in the **Asset Class** listing window, then click the --> push button.
12. Click [OK].

Assignments Form



Assets Folder - Assignments Form

Form Element	Type	Comment
Scan ID	numeric	Displays the assets scan ID. If you click [Search], you can enter the scan ID you want to search.
Name	text	Displays the name of the asset. If you click [Search], you can enter the name of the asset you want to search.
Type	drop-down list	Displays the type of asset. If you click [Search], you can enter the type of asset you want to search.
Subtype	drop-down list	Displays the subtype of the asset. If you click [Search], you can enter the subtype of the asset you want to search.
Listing window	display	Displays a list of cardholders who are currently or have been assigned to the selected asset. You can choose the number of entries you want listed by selecting **Show Assignments X Days Past** from the **Asset** menu.
Last Name	text	When you select the [Search] button, enter the last name of a cardholder to locate the assets that have been assigned to them.
First Name	text	When you select the [Search] button, enter the first name of a cardholder to locate the assets that have been assigned to them.
Assigned	numeric	When you select the [Search] button, enter the date the asset was assigned if you want to locate the cardholder who was assigned to the asset on that date.
Unassigned	numeric	When you select the [Search] button, enter the date the asset was unassigned if you want to locate the cardholder who was unassigned to the asset on that date.
Photo	display	Displays a photo of the asset if one was captured in the Multimedia Capture module.

Assets Folder - Assignments Form (Continued)

Form Element	Type	Comment
Last Access	display	Displays the date and time of the assets last access.
Assign Asset/ Assign To	push button	Displays the name of the asset currently displayed in the Cardholders folder. If no name is displayed, when selected the Cardholders folder is launched from where you can search for and select the cardholder you wish to assign to the asset.
Search	push button	Used to locate a cardholder or asset assignment record.
Last Search	push button	Click on this button the display the findings of the previous search.
	push button	Moves to the first matching record.
	push button	Moves 10 matching records back.
	push button	Moves to the previous matching record.
	push button	Moves to the next matching record.
	push button	Moves 10 matching records forward.
	push button	Moves to the last matching record.
Record count	numeric	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Add	push button	This button is not used.
Modify	push button	This button is not used.
Delete	push button	This button is not used.
Print	push button	This button is not used.

Assignments Form Procedures

Assign a Cardholder to an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the record of that asset that you want to assign.
2. If the Cardholders folder was already open and a cardholder record displayed, proceed to 3. If not, click [Assign Asset] to launch the Cardholders folder.
3. On the Cardholders folder, retrieve the record of the cardholder you want to assign to the asset. On the Assignments form of the Assets folder, the name of the cardholder will appear in the [Assign To] push button.
4. Click [Assign To] to assign the selected asset to the selected cardholder. The name of the cardholder will appear in the listing window.

Unassign an Asset

Note: This procedure does not apply to view only workstations.

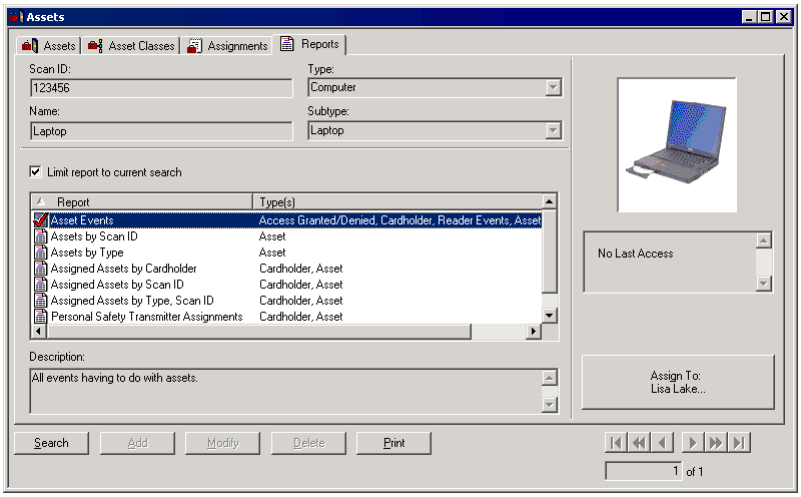
1. Locate the record of the asset that you want to unassign.
2. In the listing window, select the name of the cardholder who is currently assigned to the asset. The entry of the cardholder who is assigned will not list an **Unassigned** Date.
3. Right-click on the cardholder entry you selected and choose **Unassign Asset** from the menu. The **Unassigned** field will be updated to the current date.

Search for a Cardholder Assigned to an Asset

1. Locate the asset record that you want to look up a cardholder for.
2. In the listing window, select the name of the cardholder you want to look up.
3. Right-click on the cardholder entry you selected and choose **Find Cardholder** from the menu. The Cardholders folder will display the record of the cardholder you selected.

Reports Form

Note: The Reports form is not available in view/edit only workstations or in the Alarm Monitoring application.



Assets Folder - Reports Form

Form Element	Type	Comment
Scan ID	numeric	Displays the scan ID of the selected asset.
Name	text	Displays the name of the selected asset.
Type	drop-down list	Displays the type of the selected asset.
Subtype	drop-down list	Displays the subtype of the selected asset.
Listing window	display	Displays a list of the types of reports that can be previewed and/or printed. An icon precedes each entry.
Limit report to current search	checkbox	Select this checkbox if you want to limit this report to the search that you just completed.
Description	display	Displays a description of the report type you selected from the listing window.
Filename	display	Displays the file name of the report type.
Photo	display	Displays the captured photo of the currently selected asset.
Last Access	display	Displays the date and time of the asset's last access.
Assign Asset/ Assign To	push button	Displays the name of the cardholder currently displayed in the Cardholders folder. If no name is displayed, when selected the Cardholders folder is launched from where you can search for and select the cardholder you wish to assign to the selected asset.

Assets Folder - Reports Form (Continued)

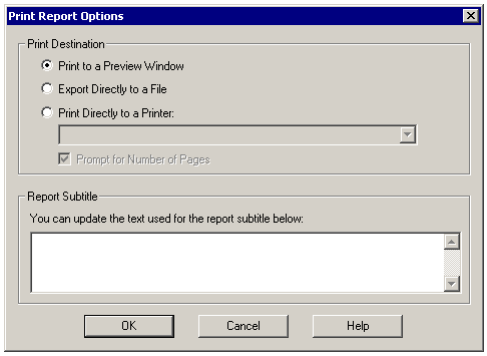
Form Element	Type	Comment
Search	push button	This button is not used.
Add	push button	This button is not used.
Modify	push button	This button is not used.
Delete	push button	This button is not used.
Print	push button	This button launches the Report Print Options window from where you can preview, print or export a report.
	push button	Moves to the first matching record.
	push button	Moves 10 matching records back.
	push button	Moves to the previous matching record.
	push button	Moves to the next matching record.
	push button	Moves 10 matching records forward.
	push button	Moves to the last matching record.
Record count	numeric	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Close	push button	Closes the Assets folder.

Reports Form Procedures

Run an Asset Report

Note: This procedure does not apply to Alarm Monitoring.

1. In the listing window, select the type of report you want to run.
2. Select the **Limit report to current search** checkbox if you want to limit this report to the search that you just completed.
3. Click [Print]. The Print Report Options window will be displayed.



4. Choose a Print Destination and if you want, update the text used for the report subtitle.
5. Click [OK].
   - If you chose the **Print Directly to a Printer** radio button, select a printer from the drop-down list. If you select the **Prompt for Number of Pages** checkbox, the Print window will be displayed where you can select print range, number of copies and whether or not to collate your report.
   - If you chose the **Export Directly to a File** radio button, the Export window will be displayed. Choose the report Format and Destination from the drop-down lists. Depending on what you chose, enter the destination and format information in the corresponding window, then click [OK].
   - If you chose the **Print to a Preview Window** radio button, an asset report print preview window will be displayed from where you can view the selected report on the screen. For more information refer to the Report Print Preview Window chapter in the System Administration User Guide.

Chapter 17: Print Report Options Window

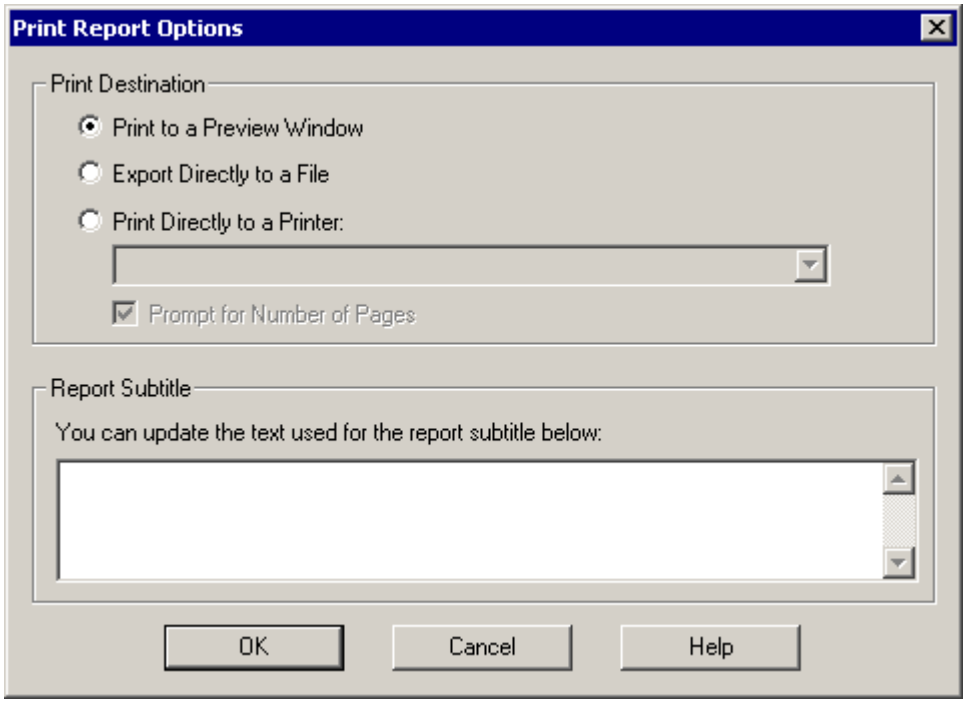
From the Print Report Options window, you can:

- Choose a destination for the report. Choices include:
  - Preview Window (the default)
  - Direct Export to a File
  - Directly to a Printer
- Update the subtitle used for the report

Toolbar Shortcut

This window is displayed by clicking the [Print] button on the Reports form or the Print toolbar button while a report is displayed.

Print Report Options Window



Print Report Options Window Field Table

Print Report Options Window

Form Element	Type	Comment
Print Destination	section	Includes the **Print to a Preview Window, Export Directly to a File** and **Print Directly to a Printer** radio buttons. Also includes the **Printer** drop-down list and the **Prompt for Number of Pages** checkbox.
Print to a Preview Window	radio button	If selected, the Report Print Preview window will be displayed when the [OK] button is clicked. In the Report Print Preview window, you can view the selected report on the screen. For more information, refer to Chapter 18: Report Print Preview Window on page 303.
Export Directly to a File	radio button	If selected, the Export window will be displayed when the [OK] button is clicked. Choose the report Format and Destination from the drop-down lists. Depending on what you choose, enter the destination and format information in the corresponding window, then click [OK].
Print Directly to a Printer	radio button	If selected, also select a printer from the Printer drop-down list. If you select the **Prompt for Number of Pages** checkbox, the Print window will be displayed where you can select the print range, number of copies and whether or not to collate your report.
Printer drop-down list	drop-down list	Select a printer in this field for the report to be printed on. This field is enabled for selection only when the **Print Directly to a Printer** radio button is selected. All printers currently configured for use are listed.
Prompt for Number of Pages	checkbox	This field is enabled for selection only when the **Print Directly to a Printer** radio button is selected. If selected, the Print window will be displayed where you can select the print range, number of copies and whether or not to collate your report.
Report Subtitle	section	Includes the **Report Subtitle** textbox.
Report Subtitle textbox	textbox	Type the text here that will be displayed as the subtitle on the report.
OK	push button	Prints the report using the options you selected.
Cancel	push button	Closes the Print Report Options window without printing the report.
Help	push button	Displays online help for this form.

Print a Report

1. Select a report from within the Reports folder. Reports are also available in the Cardholders folder (Reports form) and the Assets folder (Reports form). You can use this procedure to print those reports as well.

Notes:

The report form is available from within the Reports folder, Cardholders folder and Assets folder for System Administration and ID CredentialCenter.

The report form is only available from the Cardholders folder in Alarm Monitoring. (**View** menu > **Badge Info** > Reports form/tab)

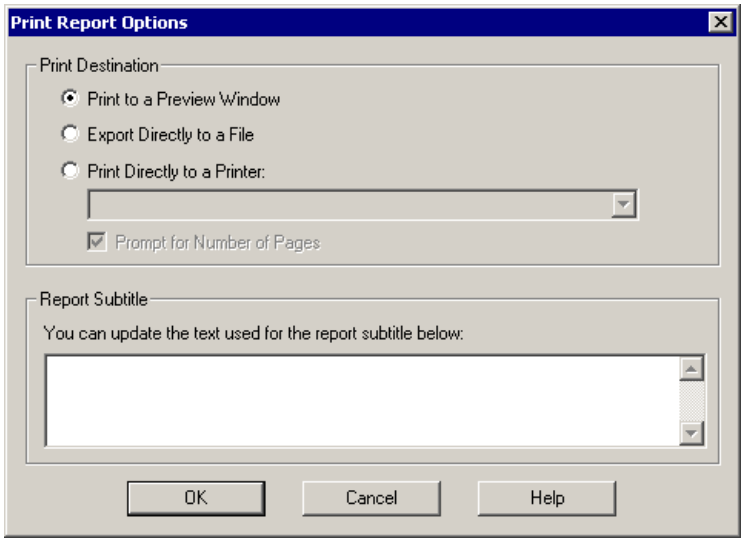
The availability of the Reports folder is subject to licensing restrictions.

2. Select additional criteria if you want the report to include only a specific range of data.
3. Click one of the following:

Toolbar Shortcut

- The Print button on the Main toolbar
- [Print] button on the form

4. The Print Report Options window opens.



In the **Print Destination** section, select whether to print to a preview window, export directly to a file or print directly to a printer.

5. If you selected **Print Directly to a Printer** in the Print Destination section, select a printer in the drop-down list and choose whether to **Prompt for Number of Pages**.

Note:

If the linkage server is running under a local system account it may not have permission to access a network printer (depending on its configuration). If this is the case you must select a local or default network printer. Contact

your System Administrator to determine what account the linkage server is running under and the printers it can access.

---

6. In the Report Subtitle section, type the report subtitle. The subtitle will be displayed below the report title on the report.
7. Click [OK]. The options selected in the Print Destination section will determine where the report is sent.

Chapter 18: Report Print Preview Window

Toolbar Shortcut

If you click [Preview] or [Print Preview] while a report form is displayed, the report is automatically printed to the Report Print Preview window.

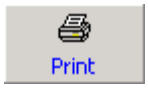
Previewing a report is done in a window. This allows you to preview multiple reports at the same time. It also means that while the report is processing, you can do other work. From the Report Print Preview window, you can:

- View an on-screen report created in the Reports folder.
- View an on-screen report created in the Cardholders folder (Reports form), The Visits folder (Reports form) or the Assets folder (Reports form) via the Print Report Options window.
- Print a report, save it to a file or send it over electronic mail.
- Search for any textual information in the report.

This window is displayed by:

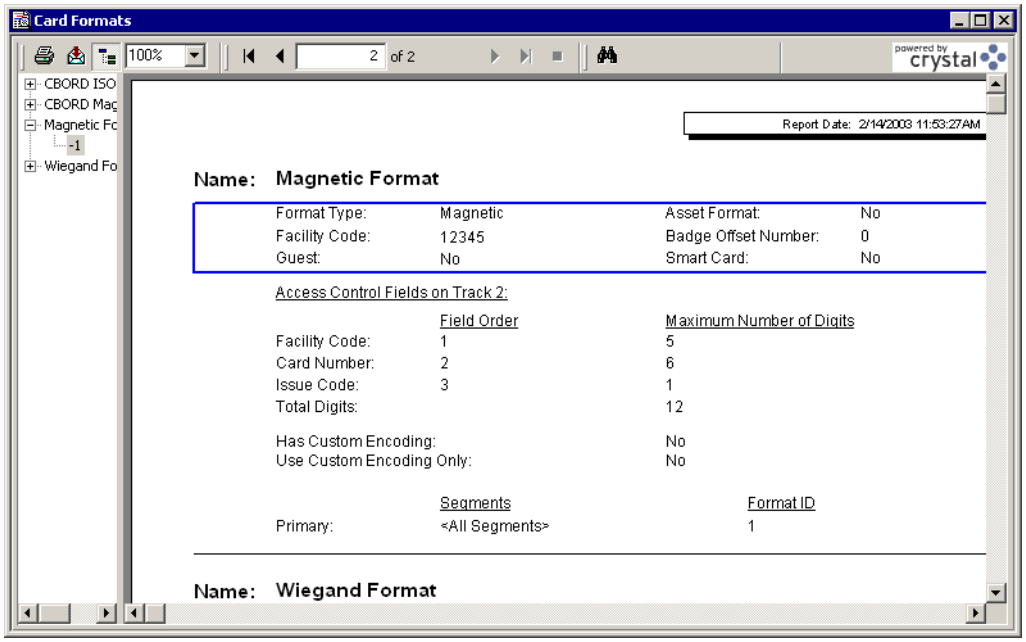
- Clicking on the [Print Preview] button on any form in the Reports folder.
- Clicking on the Print Preview toolbar button when a report is selected on a form in the Reports folder.

Toolbar Shortcut



- Clicking [Print] on the form, selecting the **Print to a Preview Window** radio button on the Print Report Options window, then clicking the [OK] button. (This is how the Report Print Preview form can be viewed from the Reports form in the Cardholders folder, the Visits folder or the Assets folder.)

Report Print Preview Window



Report Print Preview Window Field Table

Report Print Preview Window

Form Element	Type	Comment
Report navigation tree	display	The display in the left portion of the Report Print Preview window. The report navigation tree lists the records contained in the report, in a hierarchical arrangement. The information is content-sensitive. The report type determines the entries in the tree. For example, the default “User Transaction Log” report is arranged in date order, so the tree will contain a list of dates. The tree for the default “Text Instructions” report lists alarms. The “Access and Denials, by Reader” report has an entry for each queried reader, with subentries by event date. If the tree has branching entries, you can expand the branches of the tree. When you click an entry in the tree, you move to that section or record in the report. When a section or record is selected via the report navigation tree, that section or record will appear in the preview window with a blue box border. For more information, refer to Preview and Print a Report on page 306.
Preview window	display	The display in the right portion of the Report Print Preview window. The preview window displays up to one full page of the report, depending upon the zoom level set.
	push button	Click to displays a Print window from where you can select the page range and number of copies to print, then initiate report printing.
	push button	Click to export the report to a file or to your organization’s electronic mail system.
	push button	Click to toggle the display of the report navigation tree on or off.
Zoom	drop-down list	From this drop-down list, you can select the magnification level of the preview window contents, with respect to the actual size. Choices include 400%, 300%, 200%, 150%, 100%, 75%, 50%, 25%, Page Width and Whole Page. Selecting either Page Width or Whole Page displays the corresponding percentage in this field. You can also type a number directly into this field, but you must then either press <Tab> or click outside of the field for the number to take effect.
	push button	Click to move to the first page of the report.
	push button	Click to move to the previous page of the report.
Page count	display	This display indicates the page number of the currently displayed page, followed by the total page count for the report. For example: “2 of 4.”
	push button	Click to move to the next page of the report.

Report Print Preview Window (Continued)

Form Element	Type	Comment
	push button	Click to move to the last page of the report.
	push button	Click to terminate the report building process. This button is especially useful if the report is lengthy and you want to view only part of it.
	push button	Click to display the Search window from where you can perform a text search of the report. When you enter text in the **Find what** field (in the Search window) and click [Find Next], the view jumps to the first occurrence of the requested text or a message is displayed if no match was found.

Report Print Preview Window Procedures

Preview and Print a Report

1. Select a report from within the Reports folder.

Note: Reports are also available on the Reports form in the Cardholders folder, Visits folder and Assets folder. However, the Print Preview toolbar button and the [Preview] button on the form are disabled or "grayed out." Instead, the Print toolbar button or the [Print] button on the form are used to preview and print reports from these forms. For more information, refer to Print a Report on page 299.

---

2. Select additional criteria if you want the report to include only a specific range of data.
3. Click one of the following:

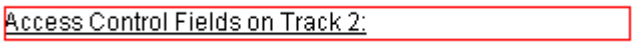
Toolbar Shortcut

- The Print Preview button on the **Main** toolbar.
- The [Print] button, select the **Print to a Preview Window** radio button and then click [OK].
- The [Preview] button on the form.

4. If the chosen report has been password-protected, type the correct password when prompted to do so, then click [OK].
5. The Report Print Preview window is displayed.
   - On the left, the report navigation tree may have branching entries.
     - If the tree has branching entries, expand that branch of the tree.
     - Click an entry in the tree to move to that section or record in the report. When a section or record is selected via the report

navigation tree, that section or record will appear in the preview window with a blue box border. For example:

- On the right, the preview window will show the first page of the report as it will look when it is printed. Click a section or record in the preview window. When a section or record is selected in the preview window, that section or record will appear in the preview window with a red box border. For example:



- Click and drag the split bar to resize the report navigation tree and the preview window relative to each other.
- Click the button to hide the report navigation tree and maximize the space used for the preview window.

6. Use the , , and buttons to view other pages of the report.
7. Select an option from the zoom drop-down list to change the size of the display. You can instead type a number directly into this field, but you must then either press <Tab> or click outside of the field for the number to take effect.
8. To save the report to a file on your computer or to send the report to someone using your company's electronic mail system, select the button. The Export window is displayed.
   - Select the format that you want to send the report in from the **Format** drop-down list.
   - In the **Destination** drop-down list, you can choose to export the report to an application, a disk file, an exchange folder, a Lotus Notes database or your electronic mail system (if you have one).
   - Click [OK] and follow the instructions
9. To print the report from within the Report Print Preview window:
   a. Click the button. The Print window is displayed from where you can select which pages to print and the number of copies.
   b. Select one of the following:
      - The **All** radio button to print the entire report without user intervention.
      - The **Pages** radio button and enter a page range.
   c. A message box will be displayed to indicate the status of the print operation.

Search a Report for Specific Information

1. To search through the report for specific information, click the button.
2. The Search window is displayed. In the **Find what** field, type the word, contiguous words or number you wish to locate in the report.

Note: The search is not case-sensitive.

---

3. Click [Find Next].
4. One of two things will happen:
   - If the requested information was found, the preview window display will move to the first occurrence of it.
   - If the information is not contained in the report, a message box will be displayed.
5. If the requested information was found, click [Find Next] to move through successive occurrences of it.

Chapter 19: Guard Tour

Guard Tour Overview

Guard tour provides a guard (a cardholder who has been specifically chosen to conduct a tour) with a defined set of tasks that must be performed within a specified period of time. Typical tasks include swiping a card at a checkpoint access reader or turning a key connected to an alarm panel input.

Checkpoints are designated stops along a tour.

Guard tour records the location and timestamp for each checkpoint visited by the tour guard. The *Checkpoint Time* represents the time it should take to reach a particular checkpoint. All checkpoints have minimum and maximum checkpoint times. A guard tour event is generated if a checkpoint is missed, reached early, on time, late, out of sequence or overdue.

A late event means the checkpoint was reached after its maximum time expired. An overdue event means the checkpoint has not yet been reached.

A tour is considered complete when one of the following actions occurs:

- All of the checkpoints on the tour are reached, even if they are reached out of sequence or some checkpoints are missed
- The tour is acknowledged as complete at a monitoring station
- The tour is terminated at a monitoring station

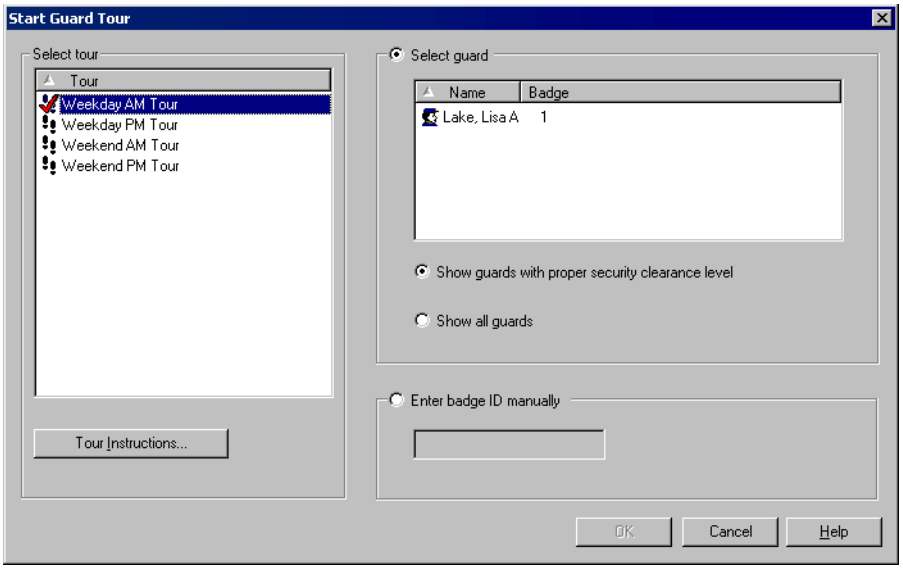
Note: System Administrator procedures to set up a Guard Tour are located in the Guard Tour Folder chapter in the System Administration User Guide.

Launch a Guard Tour

1. Start the Linkage Server by clicking the Start button, then selecting **Programs** > **B.A.S.I.S. ET** > **Linkage Server**.
2. Open the Select Guard Tour window by completing one of the following:
   - From the **Control** menu, select **Guard Tour > Launch**.

Toolbar Shortcut

- Click the down arrow on the Guard Tour toolbar button and select **Launch Tour**.
- Right-click a tour name in the system status tree and select **Launch Tour**.



3. Select a tour in the **Tour** listing window.

Note: You can click [Tour Instructions] to see if any special instructions exist for this tour. These instructions are written when the tour is configured in System Administration.

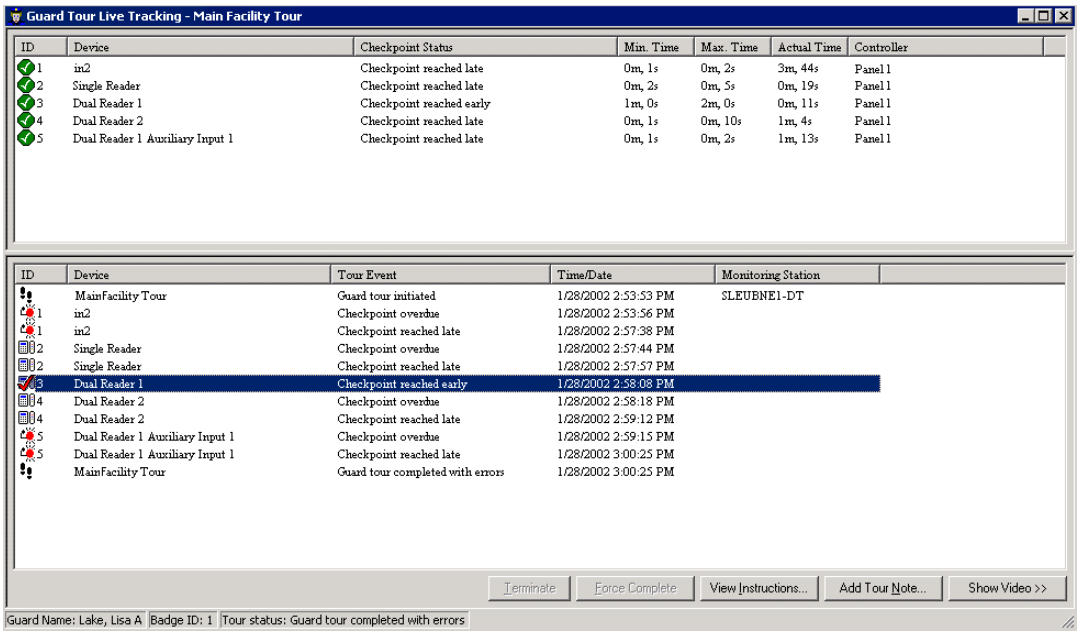
---

4. If you know the badge ID of the tour guard, select the **Enter badge ID manually** radio button and type in their ID.
   Otherwise select the **Select guard** radio button and complete the following:
   a. Select the **Show guards with proper security clearance level** radio button to limit the number of tour guards to choose from or select the **Show all guards** radio button to list all tour guards, regardless of their security clearance levels.
   b. Click a tour guard entry in the Name listing window to select it.
5. Click [OK]. The Guard Tour Live Tracking window opens.
6. At this time, the tour guard can begin the tour. As the tour progresses, the status of checkpoints and generated events display in the Guard Tour Live Tracking window. For more information, refer to Guard Tour Events Table on page 311.

Note: Checkpoints can be predecessors or successors. A predecessor checkpoint is any checkpoint occurring *before* other checkpoints on a tour. For example: a tour has three stops. Checkpoints one and two are the predecessors to checkpoint three. A successor checkpoint is any checkpoint occurring *after*

other checkpoints on a tour. For example: a tour has three stops. Checkpoints two and three are successors to checkpoint one.

7. When a tour is completed, the Guard Tour Live Tracking window displays the status of the tour and the events that were generated.


Guard Tour Live Tracking - Main Facility Tour
ID Device Checkpoint Status Min. Time Max. Time Actual Time Controller
1 in2 Checkpoint reached late 0m, 1s 0m, 2s 3m, 44s Panel 1
2 Single Reader Checkpoint reached late 0m, 2s 0m, 5s 0m, 19s Panel 1
3 Dual Reader 1 Checkpoint reached early 1m, 0s 2m, 0s 0m, 11s Panel 1
4 Dual Reader 2 Checkpoint reached late 0m, 1s 0m, 10s 1m, 4s Panel 1
5 Dual Reader 1 Auxiliary Input 1 Checkpoint reached late 0m, 1s 0m, 2s 1m, 13s Panel 1
ID Device Tour Event Time/Date Monitoring Station
MainFacility Tour Guard tour initiated 1/28/2002 2:53:53 PM SLEUBNE1-DT
1 in2 Checkpoint overdue 1/28/2002 2:53:56 PM
1 in2 Checkpoint reached late 1/28/2002 2:57:38 PM
2 Single Reader Checkpoint overdue 1/28/2002 2:57:44 PM
2 Single Reader Checkpoint reached late 1/28/2002 2:57:57 PM
3 Dual Reader 1 Checkpoint reached early 1/28/2002 2:58:08 PM
4 Dual Reader 2 Checkpoint overdue 1/28/2002 2:58:18 PM
4 Dual Reader 2 Checkpoint reached late 1/28/2002 2:59:12 PM
5 Dual Reader 1 Auxiliary Input 1 Checkpoint overdue 1/28/2002 2:59:15 PM
5 Dual Reader 1 Auxiliary Input 1 Checkpoint reached late 1/28/2002 3:00:25 PM
MainFacility Tour Guard tour completed with errors 1/28/2002 3:00:25 PM
Terminate
Force Complete
View Instructions...
Add Tour Note...
Show Video >>
Guard Name: Lake, Lisa A
Badge ID: 1
Tour status: Guard tour completed with errors

)

Guard Tour Events Table

Event	Description
Guard Tour Initiated	Generated when a tour is launched from a monitoring station.
Guard Tour Completed	Generated when all checkpoints on a tour have a “Checkpoint Reached on Time” status. Otherwise, a “Guard Tour Completed with Errors” event is generated.
Guard Tour Completed with Errors	Generated when the last checkpoint has been reached but one or more checkpoints were not reached on time or were missed altogether.
Guard Tour Cancelled	Generated when the scheduled automatic guard tour is cancelled before the tour was started.
Guard Tour Terminated	Generated when the [Terminate] button is selected in the Guard Tour Live Tracking window.
Checkpoint reached out of Sequence	Generated when a checkpoint is hit ahead of schedule on a tour (i.e., it is supposed to be hit later in a tour).
Checkpoint Missed	When a checkpoint is assigned a status of “Checkpoint reached out of sequence”, the “Checkpoint Missed” event is generated for all previous checkpoints that have a status of “Checkpoint Not Reached.”

Guard Tour Events Table (Continued)

Event	Description
Checkpoint Reached on Time	Generated when a checkpoint is hit between its minimum and maximum checkpoint times. **Note:** Checkpoint reached events are: • Generated for readers in all modes except “locked” and “unlocked” on Apollo panels. • Generated when any inputs that are used as checkpoints are activated.
Checkpoint Reached Early	Generated when a checkpoint is the next checkpoint on a tour and is hit before its minimum checkpoint time has elapsed. **Note:** Checkpoint reached events are: • Generated for readers in all modes except “locked” and “unlocked” on Apollo panels. • Generated when any inputs that are used as checkpoints are activated.
Checkpoint Overdue	Generated when a checkpoint’s maximum checkpoint time has elapsed and the guard has not yet arrived.
Checkpoint Reached Late	Generated for a checkpoint when its maximum checkpoint time has elapsed and it is then hit. **Note:** Checkpoint reached events are: • Generated for readers in all modes except “locked” and “unlocked” on Apollo panels. • Generated when any inputs that are used as checkpoints are activated. Readers on Apollo panels in “locked” and “unlocked” modes will not report cardholder events. Therefor, although those readers may be included within a guard tour, the status of those checkpoints will not be updated within the live tracing of the tour. Furthermore, since the status of a checkpoint reader in the “locked” or “unlocked” mode cannot be updated, tours containing such checkpoints will generate a “Completed With Errors with Errors” event when finished.

Guard Tour Live Tracking Window Buttons

Button	Function
The following table identifies the buttons available on the Guard Tour Live Tracking window	
Terminate	Stops a tour before it is completed (before all of the checkpoints have been reached). When this button is selected, a “Guard Tour Terminated” event is generated.
Force Complete	Manually completes a tour. For example, the [Force Complete] button could be used to end a tour that otherwise could not be completed because of a card that could not be swiped at a reader (a checkpoint) that was in “unlocked” mode.
View Instructions	Displays special instructions that were written for this tour when it was configured in the System Administration application.
Add Tour Note	Adds a note to an event. For example, you can add a note explaining why a particular checkpoint was reached late.
Show Video	Displays live video of the tour as it progresses. (This button is displayed only when the tour is configured to show video.

Schedule an Automatic Guard Tour Action

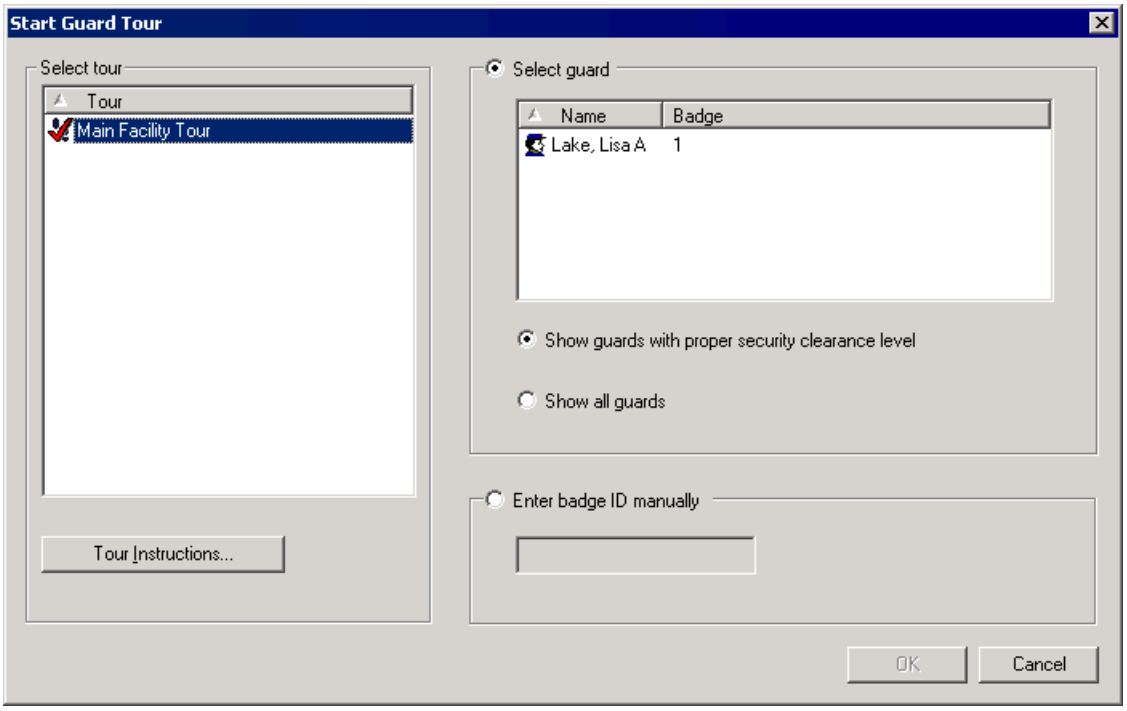
Assuming your System Administrator has configured a Guard Tour (in System Administration) you can schedule an automatic guard tour action (in Alarm Monitoring). This means that using the Scheduler you can set B.A.S.I.S. to automatically launch a Guard Tour on at a specific date and time as well as on a regular basis.

1. Open the Scheduler by clicking the Scheduler toolbar button or selecting **Scheduler** from **View** menu.
2. Click [Add].
3. The Add Action Wizard window displays. In the Category pane select **Action Types**. In the Objects pane select **Automatic Guard Tour**.
4. Click [Next].
5. The Automatic Guard Tour Properties window displays. Select a tour or tour group.
6. Select the Monitoring stations to be notified.
7. Click the Schedule tab.
8. Select the World time zone.
9. If the automatic Guard Tour is a single occurrence select the **One time** radio button and set the start date and time.
10. If the automatic Guard Tour will occur several times click the **Recurring** radio button and click [Change].
    a. Set how often you want the Guard Tour to occur and the start and end dates.
    b. Click [OK].
    c. The frequency settings display in the in the Recurring pane on the schedule tab.
11. Click [OK].

Respond to an Automatic Guard Tour

1. When an automatic Guard Tour is started, Alarm Monitoring displays a *Scheduler Action Executed* alarm and you prompts you to start the Guard Tour by displaying the following window.

2. Click [OK].
3. The Start Guard Tour window displays with the guard tour name selected. Select the guard (person) to complete the tour by either selecting the guard from the list provided or entering the guard's badge ID.

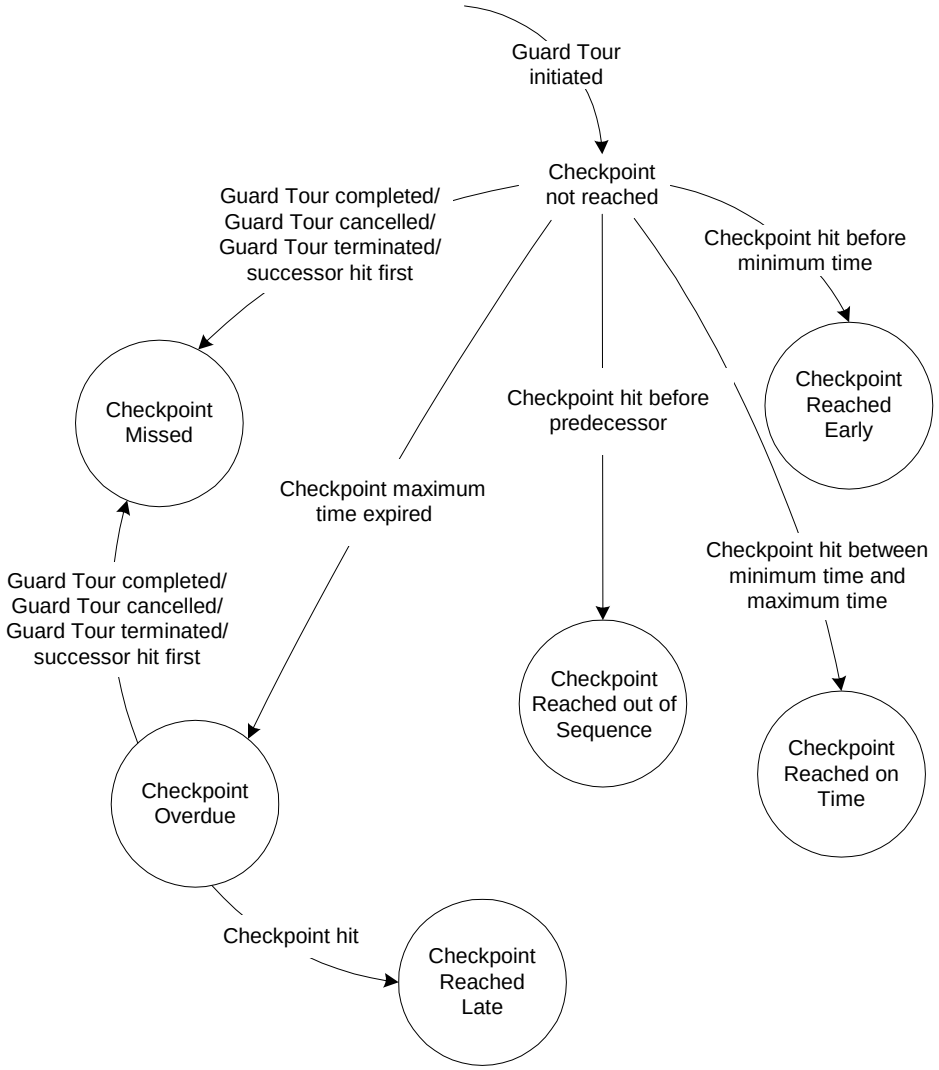


4. Click [OK].
5. While the Guard Tour is active you can monitor the Guard Tour status by selecting **Control** > **Guard Tour** > **View** from the main menu.
6. The Guard Tour Live Tracking window display information such as the badge ID of the person performing the Guard Tour, the checkpoint statuses, tour history as well as the ability to view instructions and video.

View a Guard Tour

1. Start the Linkage Server by clicking the Start button, then selecting **Programs** > **B.A.S.I.S. ET** > **Linkage Server**.
2. Open the Select Guard Tour window by completing one of the following:
   - From the **Control** menu, select **Guard Tour > Launch**.
   - Click the down arrow on the Guard Tour toolbar button and select **Launch Tour**.
3. The View Guard Tour window opens. Select the tour and click [OK].

Checkpoint Status and Events Diagram


Guard Tour initiated
Checkpoint not reached
Guard Tour completed/ Guard Tour cancelled/ Guard Tour terminated/ successor hit first
Checkpoint hit before minimum time
Checkpoint Missed
Checkpoint hit before predecessor
Checkpoint Reached Early
Checkpoint maximum time expired
Checkpoint hit between minimum time and maximum time
Guard Tour completed/ Guard Tour cancelled/ Guard Tour terminated/ successor hit first
Checkpoint Reached out of Sequence
Checkpoint Reached on Time
Checkpoint Overdue
Checkpoint hit
Checkpoint Reached Late

Chapter 20: Scheduler Folder

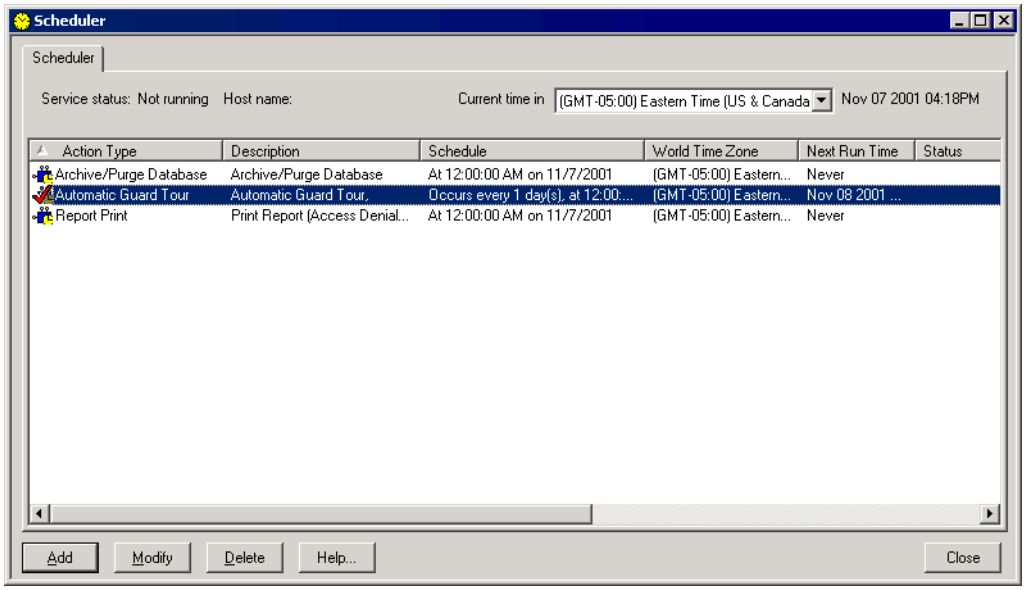
The Scheduler folder contains the Scheduler form with which you can schedule actions.

Note: Additional documentation on actions is available in the Actions appendix. For more information, refer to Appendix A: Actions on page 333.

Toolbar Shortcut

This folder is displayed by selecting **Scheduler** from the **View** menu.

Scheduler Form



Scheduler Form Field Table

Scheduler Folder - Scheduler Form

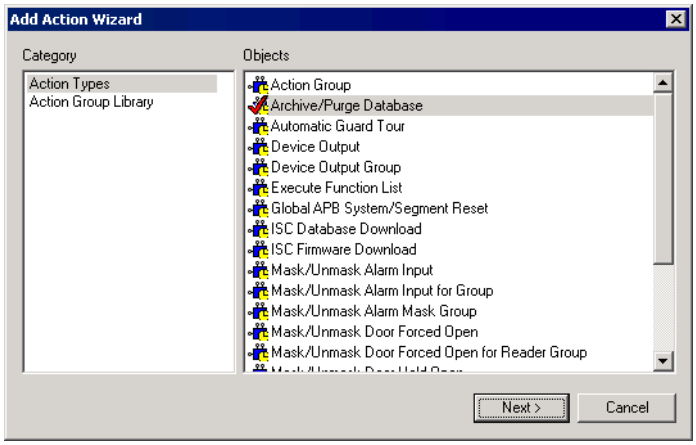
Form Element	Type	Comment
Current time in	drop-down list	When scheduling an action, select which time zone you want the action to be scheduled in. The selections in the drop-down list are listed sequentially and each includes: • The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England. • The name of one or more countries or cities that are located in that world time zone.
Listing window	display	Displays a list of all scheduled actions.
Add	push button	Click this button to open the **Add Action Wizard**.
Modify	push button	Click this button to modify the selected scheduled action.
Delete	push button	Click this button to delete the selected scheduled action.
Help	push button	Click this button to display online assistance for this form.
Close	push button	Click this button to close the Scheduler folder.

Scheduler Form Procedures

Add and Schedule an Action

1. Select **Scheduler** from the **View** menu. The Scheduler folder opens.
2. Click [Add]. The **Add Action Wizard** opens.

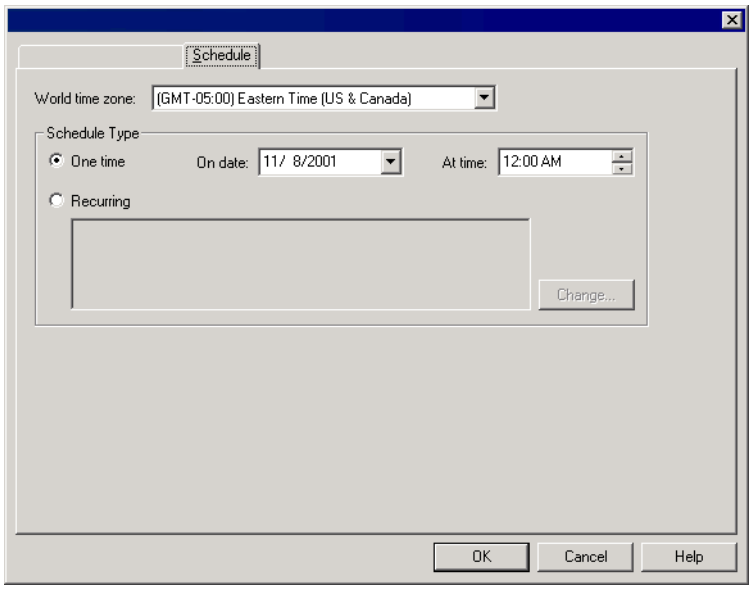
Note: You can also display the **Add Action Wizard** by right-clicking anywhere on the Scheduler form and selecting the **Add Action** menu option.



3. Select either “Action Types” or “Action Group Library” from the **Category** listing window.
   - When “Action Types” is selected, the **Objects** listing window lists all available action types.
   - When “Action Group Library” is selected, the **Objects** listing window lists all action groups which have been either created in or saved to the

action group library. For more information refer to the Action Group Library Folder chapter in the System Administration User Guide.

4. Click on an entry in the **Objects** listing window to select it.
5. Click [Next]. Depending on which Category/Object combination you chose in steps 3 and 4, a corresponding action properties window will open.
   For example, if you selected "Action Types" in the **Category** listing window and "Archive/Purge Database" in the **Objects** listing window, then the **Archive/Purge Database Properties** window would open.
6. Click the Schedule tab. The Schedule form is displayed.
   The Schedule form is the same in every action properties window that is accessed via the Scheduler folder.



7. From the **World time zone** drop-down list, select which time zone you want the action to be scheduled in. The selections in the drop-down list are listed sequentially and each includes:
   - The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected

world time zone is 5 hours ahead of the clock time in Greenwich, England.

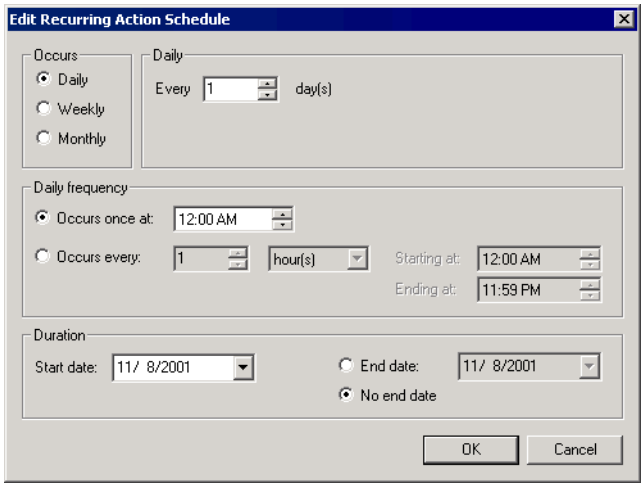
- The name of one or more countries or cities that are located in that world time zone.

8. If you want to schedule the action to occur more than once, skip this step and proceed to step 9. If you want to schedule the action to occur once:
   a. Select the **One time** radio button.
   b. In the **On date** field, the current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.

   - To select a month, click on the and navigation buttons.
   - You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
   - Navigate to a year by clicking on the displayed year to access the year spin buttons .
   - Once you have selected a month and a year, click on the day that you want the action to occur.

   c. In the **At time** field, select the time when you want this action to occur. Proceed to step 10.

9. If you want to schedule the action to occur more than once:
   a. Select the **Recurring** radio button.
   b. Click [Change]. The **Edit Recurring Action Schedule** window opens.



c. Do one of the following:

- Select the **Daily** radio button in the Occurs section if you want the action to occur on a daily basis.

  If you want the action to occur every day, in the Daily section, type the number 1 in the **Every___day(s)** field. If you want the action to occur every other day, type the number 2 and so on.

- Select the **Weekly** radio button in the Occurs section if you want the action to occur on a weekly basis.

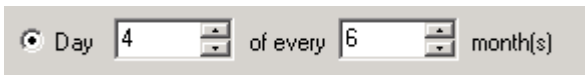
  If you want the action to occur every week, in the Weekly section, type the number 1 in the **Every___week(s) on** field. If you want the action to occur every other week, type the number 2 and so on. You must also select the checkbox that corresponds with the day of the week that you want the action to occur.

  For example, if you want the action to occur every other Monday, type the number 2 in the **Every___week(s) on** field and select the **Mon** checkbox.

- Select the **Monthly** radio button in the Occurs section if you want the action to occur on a monthly basis. Then, do one of the following:

  Select the **Day___of every___month(s)** radio button and type in which day of how many months you want the action to occur.

  The following example shows an action being scheduled to occur on the 4th day of every 6th month.



  Select the **The___of every___month(s)** radio button and enter which day of how many months you want the action to occur.

The following example shows an action being scheduled to occur of the 2nd Tuesday of every 3rd month.

d. In the Daily frequency section, do one of the following:

- If you want the action to occur only once on its scheduled day(s), select the **Occurs once at___** radio button and enter a time.

  The following example shows an action being scheduled to occur at 12:00 PM.

- If you want the action to occur more than once on its scheduled day(s), select the **Occurs every___Starting at___Ending at___** radio button and enter the hours that you want the action to occur.

The following example shows an action being scheduled to occur every 2 hours, starting at 9:00 AM and ending at 5:00 PM.

e. Enter the action's **Start date**. The current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.

- To select a month, click on the and navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
- Navigate to a year by clicking on the displayed year to access the year spin buttons .
- Once you have selected a month and a year, click on the day that you want the action to begin occurring.

f. Enter the action's **End date**. The current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.

- To select a month, click on the and navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.

- Navigate to a year by clicking on the displayed year to access the year spin buttons .
- Once you have selected a month and a year, click on the day that you want the action to stop occurring.

Note: You do not have to select an end date. If you do not want to set an end date, select the **No end date** radio button.

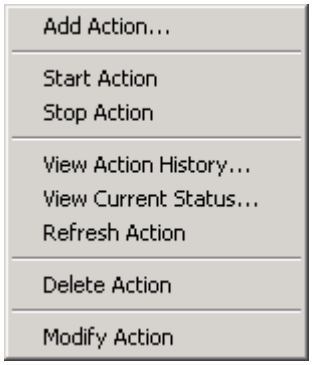
---

g. Click [OK].

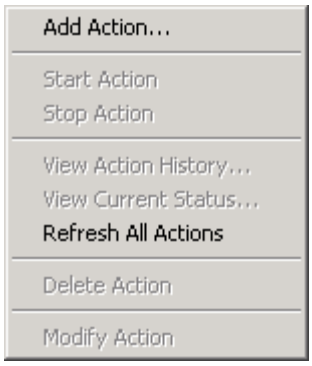
10. Now you must configure the action that you have just scheduled. Select the tab to the left of the Schedule tab (this tab will correspond to the specific action properties window which you are viewing). For more information, refer to Appendix A: Actions on page 333.

Display the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.



Note: If you right-click anywhere on the Scheduler form when a scheduled action is not selected in the listing window, the scheduler right-click menu will look like this:



Add and Schedule an Action Using the Scheduler Right-Click Menu

1. Right-click anywhere on the Scheduler form. The scheduler right-click menu is displayed.
2. Select the **Add Action** menu option. The **Add Action Wizard** opens.
3. Proceed to step 3 of the "Add and Schedule an Action" procedure in this chapter.

Start an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Start Action** menu option to start the selected action immediately.

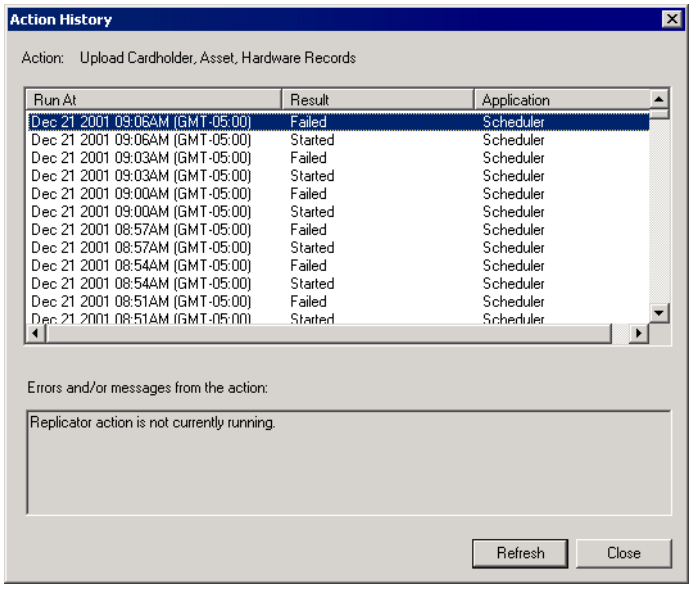
Stop an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Stop Action** menu option to stop the selected action immediately.

View Action History

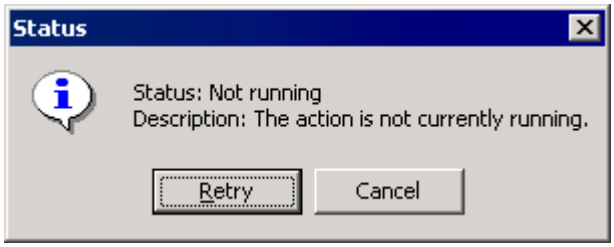
1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **View Action History** menu option. The Action History window opens and the name of the action, when the action was run, the result, the

application and any errors or messages that resulted from the action are all displayed.


Action History
Action: Upload Cardholder, Asset, Hardware Records
Run At
Result
Application
Dec 21 2001 09:06AM (GMT-05:00) Failed Scheduler
Dec 21 2001 09:06AM (GMT-05:00) Started Scheduler
Dec 21 2001 09:03AM (GMT-05:00) Failed Scheduler
Dec 21 2001 09:03AM (GMT-05:00) Started Scheduler
Dec 21 2001 09:00AM (GMT-05:00) Failed Scheduler
Dec 21 2001 09:00AM (GMT-05:00) Started Scheduler
Dec 21 2001 08:57AM (GMT-05:00) Failed Scheduler
Dec 21 2001 08:57AM (GMT-05:00) Started Scheduler
Dec 21 2001 08:54AM (GMT-05:00) Failed Scheduler
Dec 21 2001 08:54AM (GMT-05:00) Started Scheduler
Dec 21 2001 08:51AM (GMT-05:00) Failed Scheduler
Errors and/or messages from the action:
Replicator action is not currently running.
Refresh
Close

View the Current Status of an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **View Current Status** menu option. A message similar to the following will be displayed:



Refresh an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Refresh Action** menu option. The listing window will be updated to display the most current information for the selected action.

Refresh all Actions

1. Right-click anywhere on the Scheduler form except on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Refresh All Actions** menu option. The listing window will be updated to display the most current information for all of the scheduled actions.

Delete a Scheduled Action using the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Delete Action** menu option. A confirmation message is displayed.
3. Click [Yes].

Note: Selecting the **Delete Action** right-click menu option does the same thing as selecting an action in the listing window, and then clicking [Delete] on the Scheduler form.

Modify a Scheduled Action using the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Modify Action** menu option. Depending on which action you selected in the listing window, a corresponding action properties window will open.
3. Make the changes you want to the fields. For more information, refer to Appendix A: Actions on page 333.
4. Click [OK].

Note: Selecting the **Modify Action** right-click menu option does the same thing as selecting an action in the listing window, then clicking the [Modify] button on the Scheduler form.

Appendices

Appendix A: Actions

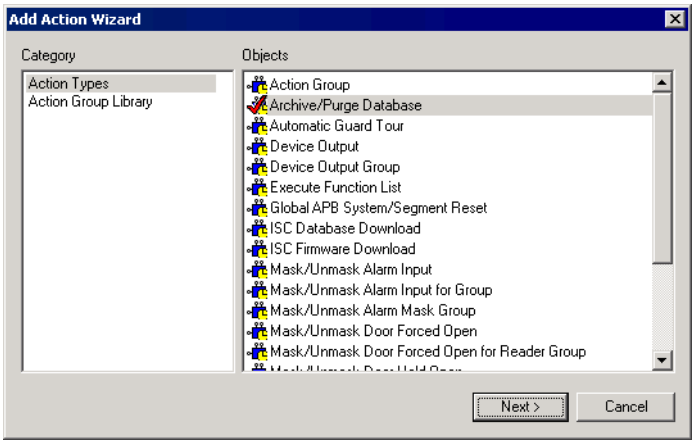
Actions Procedures

Use the Add Action Wizard

1. Click the [Add] button either:
   - In the Checkpoint Actions section of the **Tour Wizard** in the Guard Tour folder. For more information, refer to the Guard Tour Folder chapter in the System Administration User Guide.
   - On the Scheduler form of the Scheduler folder. For more information, refer to Chapter 20: Scheduler Folder on page 317.
   - On the Output Action sub-tab of the Global Linkage form in the Global I/O folder. For more information, refer to the Global I/O Folder chapter in the System Administration User Guide.
   - On the Acknowledgment Actions form in the Alarm Configuration folder. For more information, refer to the Alarm Configuration Folder chapter in the System Administration User Guide.

Note: If you have access to view multiple segments you are prompted to select a segment.

The **Add Action Wizard** Opens.



2. Choose an action **Category** and then select an action **Object**.

Note: Depending on where the **Add Action Wizard** was launched from, the objects available in the Objects listing window will vary.

3. Click [Next]. Depending on which Category/Object combination you chose in step 2, a corresponding action properties window will open.
4. Configure the action you selected in step 3. To do this, you must refer to the action properties windows sections in this chapter for information on each action properties window.
5. Repeat steps 1-4 for each action you want to assign.

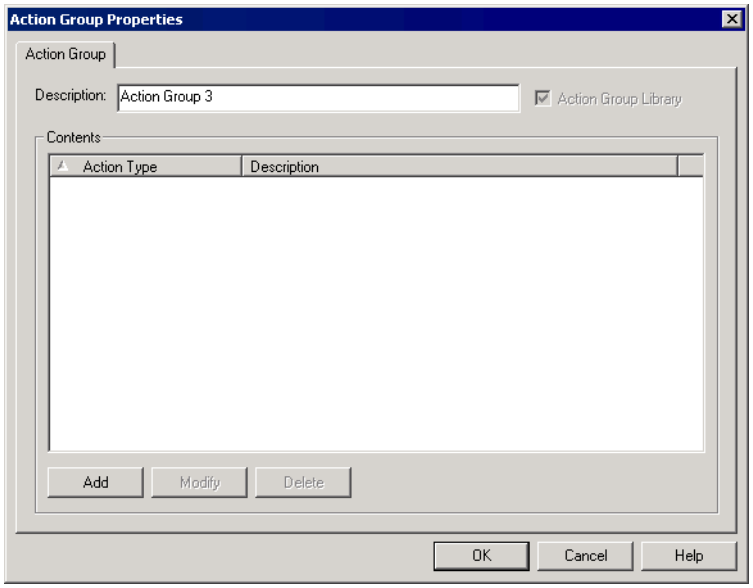
Action Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Action Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Select the “Action Group Library” **Category** and any defined action group **Object** in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Library form of the Action Group Library folder from System Administration.

Note: The open door commands will not be available for those using Recognition Source readers, because that particular reader is not in constant communication with the PIM device.

Note: For more information, refer to “Action Groups Overview” in the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Action Group Properties Window Field Table

Form Element	Type	Comment
Description	text	When adding or modifying an action group, you can enter a description of the action group that is being configured.
Action Group Library	checkbox	When selected, the action group that you are adding or modifying will be available for selection in the Action Group Library. For more information, refer to "Action Groups Overview" in the Action Group Library Folder chapter in the System Administration User Guide.
Action Type listing window	display	Displays the action types which have been assigned to the selected action group.
Add	push button	Click this button to add an action type.
Modify	push button	Click this button to modify the action type that is selected in the Action Type listing window.
Delete	push button	Click this button to delete the action type that is selected in the Action Type listing window from the selected action group.
OK	push button	Click this button to save your changes and exit out of the Action Group Properties window.
Cancel	push button	Click this button to exit the Action Group Properties window without saving your changes.
Help	push button	Click this button to display online help for this window.

Action Group Properties Window Procedures

Add an Action Group

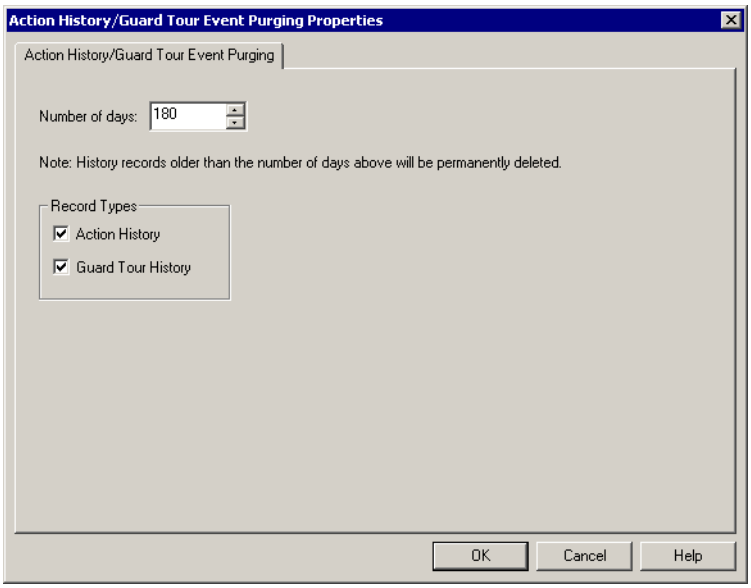
1. Display the Action Group Properties window.
2. In the **Description** field, enter a description of the action group that is being configured.
3. Select the **Action Group Library** checkbox if you want this action group to be available for selection in the Action Group Library. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.
4. Click [Add]. The Select Action Type window opens.
5. Select an action type and then click [Next]. Depending on which action type you chose, a corresponding action properties window will open.
6. Configure the action type you selected in step 5. To do this, you must refer to the action properties windows sections in this chapter for information on each action properties window.
7. Repeat steps 4-6 for each action type you want to assign to this group.
8. Click [OK].

Action History/Guard Tour Event Purging Properties Window

The Action History/Guard Tour Event Purging action allows you to create an action that will automatically delete certain records after they are a specified number of days old. For example, you can have all Guard Tour History record types deleted when they are 180 days old.

To display, do one of the following:

- Select the "Action Types" **Category** and the "Action History/Guard Tour Event Purging" **Object** in the Add Action Wizard. For more information refer to Use the Add Action Wizard on page 333.
- Click the [Add] button on the Action Group Library form of the Action Group Library folder from System Administration.



Action History/Guard Tour Event Purging Properties Window

Form Element	Type	Comment
Number of Days	spin button	The history records older than the number of days selected will be permanently deleted when the action runs.
Action History	check box	Select this check box if you want Action History records deleted that are older than the **Number of days** setting.
Guard Tour History	check box	Select this check box if you want Guard Tour History records deleted that are older than the **Number of days** setting.
OK	push button	Click this button to add the action and exit out of the Action History/ Guard Tour Event Purging Properties window.
Cancel	push button	Click this button to exit the Action History/Guard Tour Event Purging Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Action History/Guard Tour Event Purging Properties Window Procedures

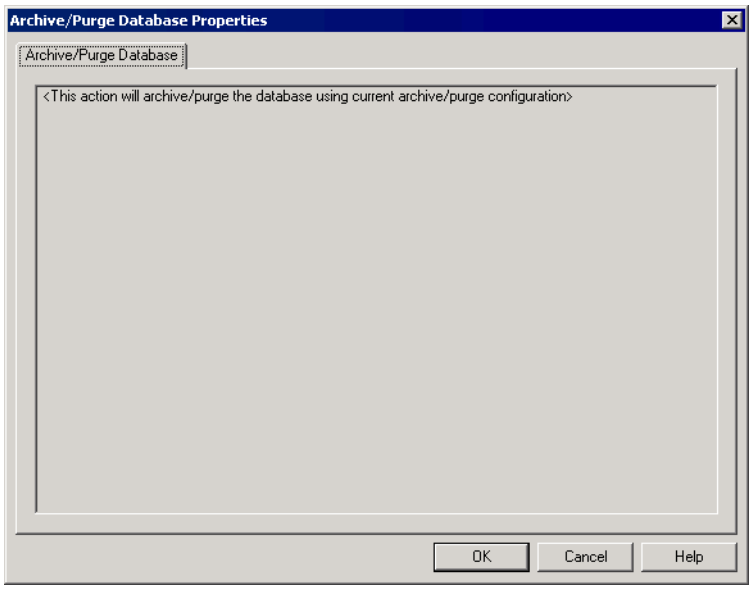
Add an Action History/Guard Tour Event Purging Action

1. From the **Administration** menu, select **Action Group Library**.
2. Click [Add] on the Action Group Library form. The Action Group Properties window opens.
3. Click [Add] on the Action Group Properties window.
4. Click Action History/Guard Tour Event Purging. A checkmark appears next to the name.
5. Click [Next]. The Action History/Guard Tour Event Purging Properties window appears.
6. Choose the type of records you want to delete and the set number of days you want them deleted after.
7. Click [OK].

Archive/Purge Database Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Archive/Purge Database” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Archive/Purge Database Group** form the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Archive/Purge Database Properties Window Field Table

Form Element	Type	Comment
Listing window	display	Displays the following message: "<This action will archive/purge the database using current archive/ purge configuration>"
OK	push button	Click this button to add the action and exit out of the Archive/Purge Database Properties window.
Cancel	push button	Click this button to exit the Archive/Purge Database Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Archive/Purge Database Properties Window Procedures

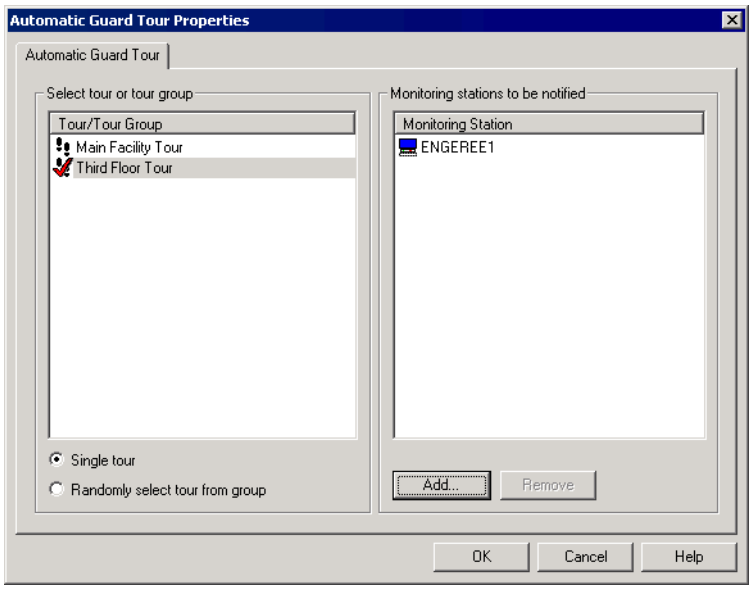
Add an Archive/Purge Database Action

1. Display the Archive/Purge Database Properties window.
2. Click [OK]. This action is now configured to archive/purge the database using your current archive/purge configurations. For more information, refer to the Archives Folder chapter in the System Administration User Guide.

Automatic Guard Tour Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Automatic Guard Tour” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Automatic Guard Tour** form the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.
- Click the [Add] button on the Scheduler form in the Guard Tour folder.



Note: If you have accessed the Automatic Guard Tour Properties window via the Scheduler folder or the Scheduler form in the Guard Tour folder, the window will contain both the Automatic Guard Tour form and the Scheduler form. You *must* refer to the Scheduler folder chapter for detailed information on how to use the Automatic Guard Tour Properties window in conjunction with Scheduler. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Automatic Guard Tour Properties Window Field Table

Form Element	Type	Comment
Tour/Tour Group listing window	display	Displays a list of the tours and tour groups which have been configured in the system. Tours and tour groups are configured in the Guard Tour folder.
Single tour	radio button	Select this radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.
Randomly select tour from group	radio button	Select this radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured as random tour lists will be listed in the Tour/Tour Group listing window. Tour groups are configured on the Tour Groups form of the Guard Tour folder. A tour group is considered a random tour list when the **Random Tour List** checkbox is selected on the Tour Groups form.
Monitoring Station listing window	display	Displays a list of the monitoring stations which are assigned to the selected tour. These monitoring stations will be notified when the automatic guard tour is scheduled to begin.
Add	push button	Click this button to display the Select Monitoring Station window and add a monitoring station to the Monitoring Station listing window.
Remove	push button	Click this button to remove the selected monitoring station from the Monitoring Station listing window.
OK	push button	Click this button to add the action and exit out of the Automatic Guard Tour Properties window.
Cancel	push button	Click this button to exit the Automatic Guard Tour Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Automatic Guard Tour Properties Window Procedures

Add an Automatic Guard Tour Action

1. Display the Automatic Guard Tour Properties window.
2. Do one of the following:
   - Select the **Single Tour** radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.
   - Select the **Randomly select tour from group** radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured

as random tour lists will be listed in the Tour/Tour Group listing window.

3. The monitoring stations that have been assigned to the selected tour or tour group will be displayed in the Monitoring Station listing window. Do one of the following:
   - If no monitoring stations have been assigned or if you want to assign an additional monitoring station, then click [Add]. The Select Monitoring Station window opens.
   - If you do not want to assign a monitoring station, proceed to step 7.
4. Click on a monitoring station to select it.
5. Click [OK]. The monitoring station you selected will be listing in the Monitoring Station listing window. All monitoring stations in the Monitoring Station listing window will, in the Alarm Monitoring application, receive a notification message when the tour is scheduled to begin.
6. Repeat steps 3-5 for each monitoring station you want to add.

Note: If you want to remove a monitoring station from the Monitoring Station listing window, click on an entry to select it and then click [Remove].

7. Click [OK].

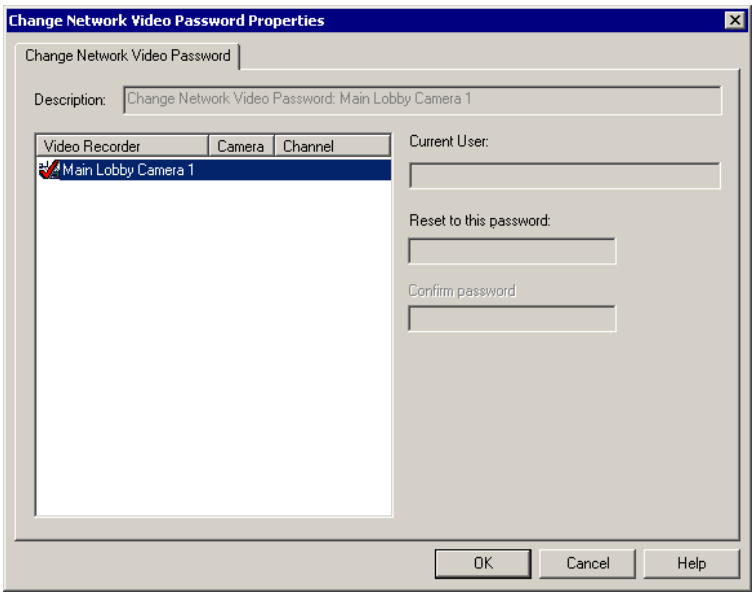
Note: If you have accessed the Automatic Guard Tour Properties window via the Scheduler folder or the Scheduler form in the Guard Tour folder, the window will contain both the Automatic Guard Tour form and the Schedule form. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Change Network Video Password Properties Window

The Change Network Video Password action allows you to schedule automatic password changes for video recorders. You can make the change a one-time event or to schedule it daily, weekly, or monthly with the Edit Recurring Action Schedule. For more information, refer to Chapter 20: Scheduler Folder on page 317.

To display, do one of the following:

- Click [Add] on the Output Action tab in the Global I/O form, and choosing Change Network Video Password.
- Click [Add] on the Scheduler form, and choosing Change Network Video Password.



Change Network Video Password Properties Window Field Table

Form Element	Type	Comment
Description	display	Names the video device you are currently changing the password for.
Listing Window	display	Lists currently defined LNVR recorders and cameras associated with them. Select the recorders and/or cameras you want to modify.
Current User	display	The name of the user account. This field automatically populates if a user name was initially populated on the Video Recorder/Camera forms.

Change Network Video Password Properties Window Field Table

Form Element	Type	Comment
Reset to this password	text field	Enter the password in the text box. The following restrictions apply: • Axis cameras all up to 10 character passwords using A through Z, a through z, 0 - 9, !, #' - ', -, ., ^, _, ~, $ • Sony cameras allow up to 16 character passwords using A through Z, a through z, 0 - 9 • LNVR recorder password length is limited by the LNVR's computer password policy, which is set by the system administrator. Valid characters are ! - ~ **Note:** In addition to these restrictions, B.A.S.I.S. includes strong password enforcement, which checks the user's password against password standards.
Confirm password	text field	Enter the password a second time for verification.
OK	push button	Adds the action and exits out of the Change Network Video Properties window.
Cancel	push button	Exits the Change Network Video Password Properties window without adding the action.
Help	push button	Displays online help for this window.

Change Network Video Password Properties Window Procedures

Schedule a One-Time Password Change

1. From the **Administration** menu select **Scheduler**.
2. Click [Add] on the Scheduler form. The Add Action Wizard window opens.
3. Select "Change Network Video Password" from the Objects listing window.
4. Click [Next]. The Change Network Video Password Properties window displays.
5. On the Schedule sub-tab, select the **One time** radio button.
6. Select the date and time you wish the password to change.
7. Click [OK].

Schedule a Recurring Password Change

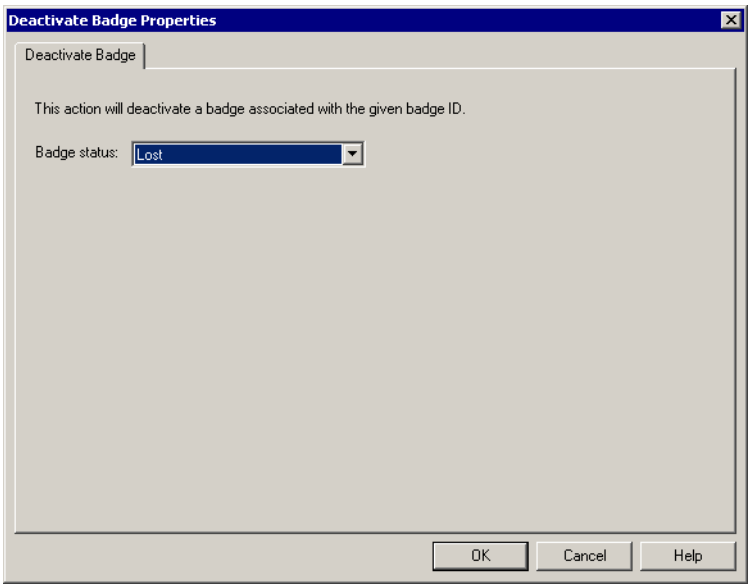
1. From the **Administration** menu select **Scheduler**.
2. Click [Add] on the Scheduler form. The Add Action Wizard window opens.
3. Select “Change Network Video Password” from the Objects listing window.
4. Click [Next]. The Change Network Video Password Properties window displays.
5. On the Schedule sub-tab, select the **Recurring** radio button.
6. Click [Change]. The Edit Recurring Action Schedule form displays.
7. Choose the time and date intervals that best suit your needs.
8. Click [OK] on the Edit Recurring Action Schedule form.
9. Click [OK] on the Change Network Video Password Properties window.

Deactivate Badge Properties Window

The Deactivate Badge action allows you to deactivate a cardholder's badge when it is either lost or returned.

To display the Deactivate Badge Properties window, click [Add] on the Output Action tab in the Global I/O form, and choose Change Network Video Password.

Note: An action of this type can only be utilized from the Global I/O. In order to execute the action, Global I/O should have a linkage configured on a device, event, and badge ID that is passed to the action at runtime.



Deactivate Badge Properties Window Field Table

Form Element	Type	Comment
Badge Status	drop down	Use to select the status of a badge that will be deactivated. Choices are Lost and Returned.
OK	push button	Click this button to add the action and exit out of the Deactivate Badge Properties window.
Cancel	push button	Click this button to exit the Deactivate Badge Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Deactivate Badge Properties Window Procedures

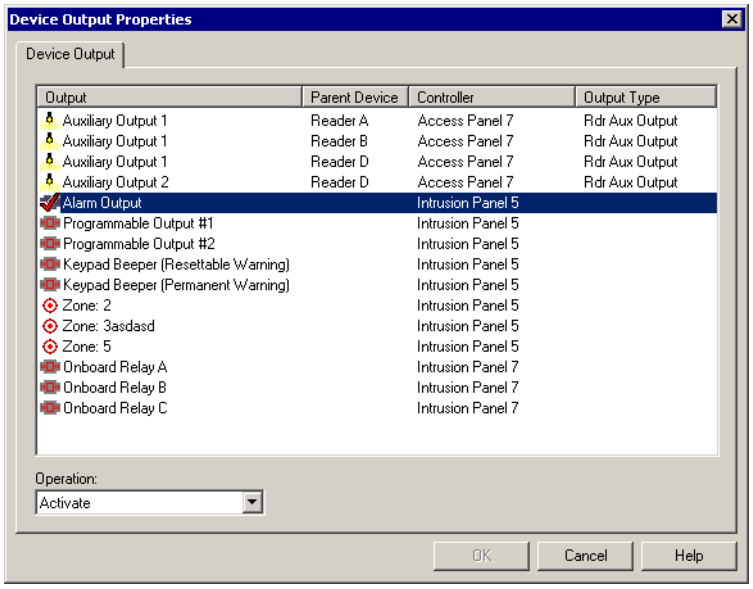
Add a Deactivate Badge Action

1. From the **Access Control** menu, select **Global I/O**. The Global Linkage form displays.
2. Click [Add].
3. Click the Output Action sub-tab.
4. Click [Add]. The Add Action Wizard window opens.
5. Select “Deactivate Badge” from the Objects listing window.
6. Click [Next]. The Deactivate Badge Properties window appears.
7. Choose the type of badge you want to deactivate.
8. Click [OK].
9. Click [OK] again.

Device Output Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Device Output” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Device Output** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Device Output Properties Window Field Table

Form Element	Type	Comment
Output listing window	display	Displays a list of available device outputs which have been configured in the system.
Activate	radio button	When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will activate. When a device output is activated, that means it is in an “on” state.
Deactivate	radio button	When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will deactivate. When a device output is deactivated, that means it is in an “off” state.
Pulse	radio button	When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will pulse (turn on and then turn off again).
Toggle	radio button	When configuring a device output as an action, select this from the drop-down menu if you want to toggle the state of the relay. For example, if the relay is on (activated), toggling deactivates it. If the relay is off (deactivated), toggling activates it. **Note:** Only offboard relays on the Radionics (7412 and 9412) intrusion panels support the toggle option.
OK	push button	Click this button to add the action and exit out of the Device Output Properties window.
Cancel	push button	Click this button to exit the Device Output Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Device Output Properties Window Procedures

Add a Device Output Action

1. Display the Device Output Properties window.
2. Click on an entry in the Output listing window to select it.
3. Do one of the following:
   - Select **Activate** from the drop-down menu if you want this action to be that the device output will activate. When a device output is activated, that means it is in an “on” state.
   - Select **Deactivate** from the drop-down menu if you want this action to be that the device output will deactivate. When a device output is deactivated, that means it is in an “off’ state.
   - Select **Pulse** from the drop-down menu if you want this action to be that the device output will pulse (turn on and then turn off again).
   - Select **Toggle** from the drop-down menu in you want this action to be that

the device output will toggle the state of the relay. For example, if the relay is on (activated), toggling deactivates it. If the relay is off (deactivated), toggling activates it.

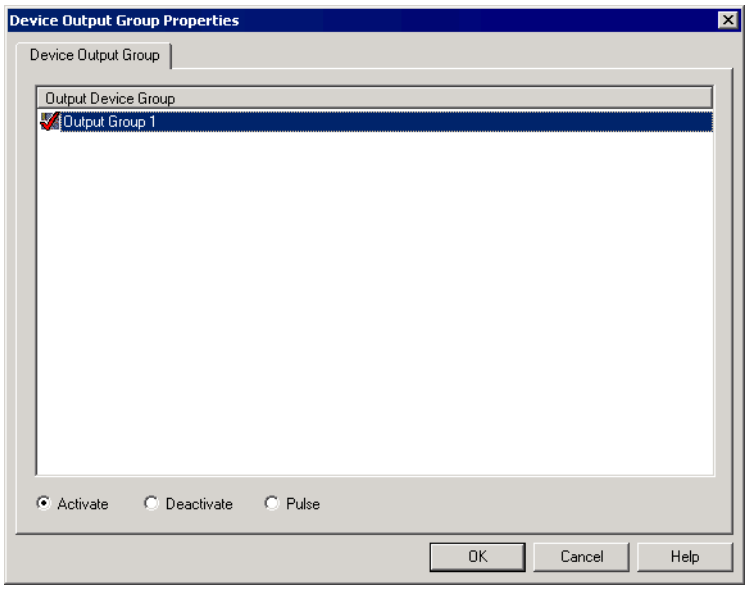
Note: Only offboard relays on the Radionics (7412 and 9412) intrusion panels support the toggle option.

- Click [OK].

Device Output Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Device Output Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Device Output Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Device Output Group Properties Window Field Table

Form Element	Type	Comment
Output Device Group listing window	display	Displays a list of available output device groups which have been configured in the system.
Activate	radio button	When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will activate. When device outputs are activated, that means they are in an “on” state.
Deactivate	radio button	When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will deactivate. When device outputs are deactivated, that means they are in an “off” state.
Pulse	radio button	When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will pulse (they will turn on and then turn off again).
OK	push button	Click this button to add the action and exit out of the Device Output Group Properties window.
Cancel	push button	Click this button to exit the Device Output Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Device Output Group Properties Window Procedures

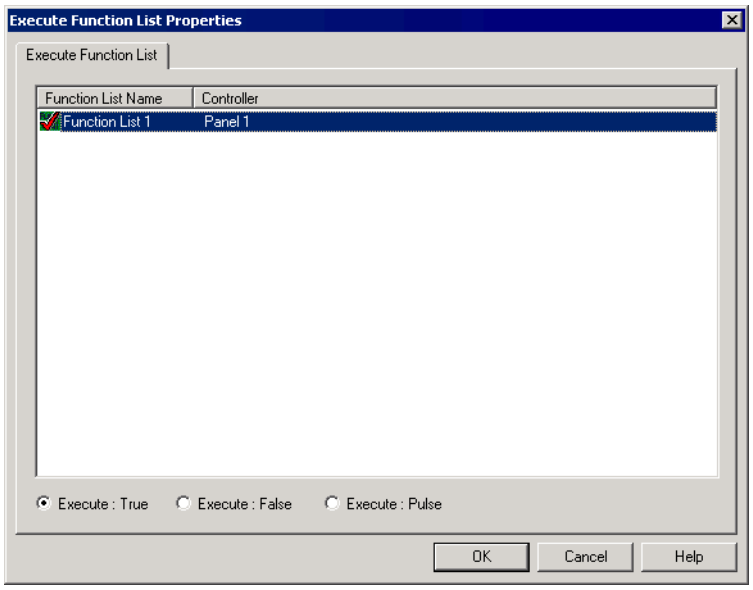
Add a Device Output Group Action

1. Display the Device Output Group Properties window.
2. Click on a group in the Output Device Group listing window to select it.
3. Do one of the following:
   - Select the **Activate** radio button if you want this action to be that the device outputs in the group will activate. When device outputs are activated, that means they are in an “on” state.
   - Select the **Deactivate** radio button if you want this action to be that the device outputs in the group will deactivate. When device outputs are deactivated, that means they are in an “off’ state.
   - Select the **Pulse** radio button if you want this action to be that the device outputs in the group will pulse (they will turn on and then turn off again).
4. Click [OK].

Execute Function List Properties Window

To display, do one of the following:

- Selecting the “Action Types”/ “Execute Function List” **Category**/**Object** combination in the **Add Action Wizard**.
- Clicking [Add] on the Action Group Properties window and selecting **Execute Function List** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Execute Function List Properties Window Field Table

Form Element	Type	Comment
Function List listing window	display	Displays a list of available function lists which have been configured in the system.
Execute: True	radio button	When configuring a function list as an action, select this radio button if you want the action to execute the function list with an argument of "True."
Execute: False	radio button	When configuring a function list as an action, select this radio button if you want the action to execute the function list with an argument of "False."
Execute: Pulse	radio button	When configuring a function list an action, select this radio button if you want the action to execute the function list with an argument of "Pulse."
OK	push button	Click this button to add the action and exit out of the Execute Function List Properties window.
Cancel	push button	Click this button to exit the Execute Function List Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Execute Function List Properties Window Procedures

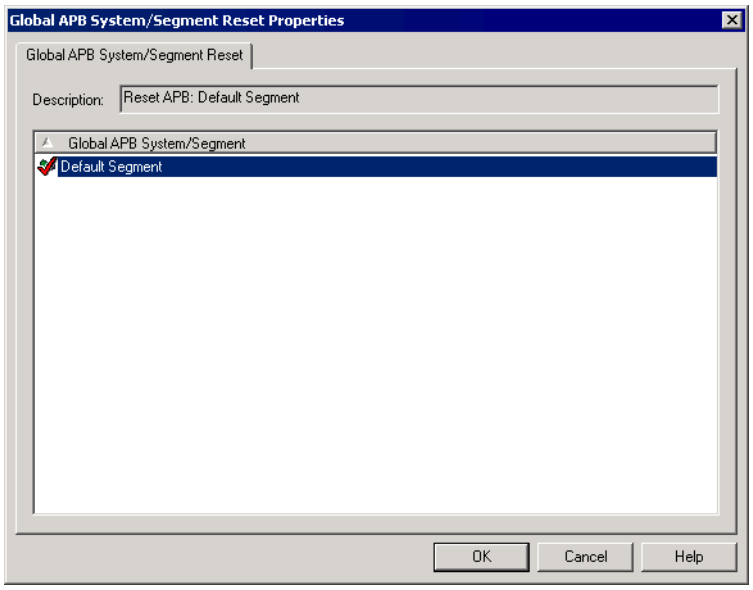
Add an Execute Function List Action

1. Display the Execute Function List Properties window.
2. Click on a function list in the Function List listing window to select it.
3. Do one of the following:
   - Select the **Execute: True** radio button if you want this action to execute the function list with an argument of "True."
   - Select the **Execute: False** radio button if you want this action to execute the function list with an argument of "False."
   - Select the **Execute: Pulse** radio button if you want this action to execute the function list with an argument of "Pulse."
4. Click [OK].

Global APB System/Segment Reset Properties Window

Displayed by clicking [Add] on the Action Group Properties window and then selecting **Global APB System/Segment Reset** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.

You can also select the “Action Types”/ “Global APB System/Segment Reset” **Category**/**Object** combination in the **Add Action Wizard**.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Global APB System/Segment Reset Properties Window Field Table

Form Element	Type	Comment
Description	text	Displays a description of the selected global APB system/segment.
Global APB System/Segment listing window	display	Displays a list of the segments available for this action.
OK	push button	Click this button to add the action and exit out of the Global APB System/Segment Reset Properties window.
Cancel	push button	Click this button to exit the Global APB System/Segment Reset Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Global APB System/Segment Reset Properties Window Procedures

Add a Global APB System/Segment Reset Action

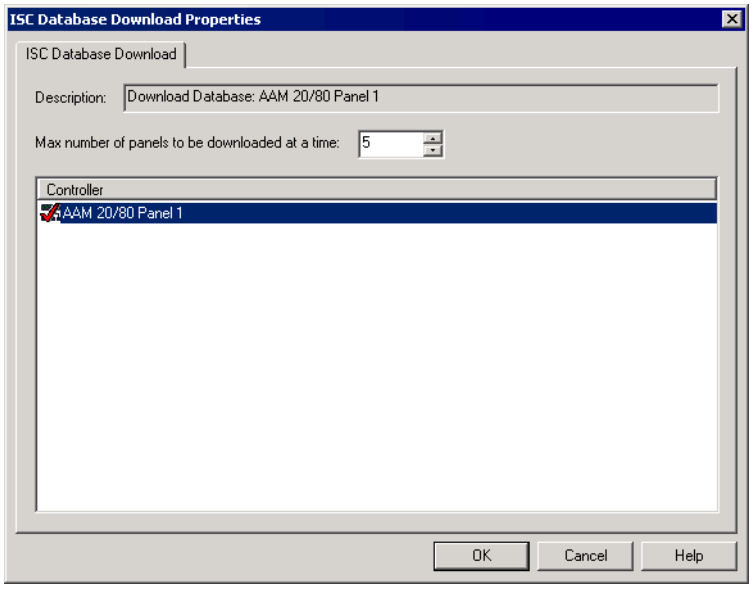
1. Display the Global APB System/Segment Reset Properties window.
2. Select a segment from the Global APB System/Segment listing window to select it.
3. Click [OK]. If segmentation is enabled, this action will reset APB for the selected segment. If segmentation is not enabled, this action will reset APB for your entire system.

Note: Global APB must be configured on your system in order to add this action.

ISC Database Download Properties Window

Displayed by clicking [Add] on the Action Group Properties window and selecting **ISC Database Download** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.

You can also select the “Action Types”/ “ISC Database Download” **Category**/ **Object** combination in the **Add Action Wizard**.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

ISC Database Download Properties Window Field Table

Form Element	Type	Comment
Description	text	Displays a description of the access panel which is selected in the Access Panel listing window. **Note:** This field only displays a description when one and only one access panel is selected.
Max number of panels to be downloaded at a time	spin buttons	When configuring a database download as an action, select the maximum number of access panels that can be downloaded at a time.
Controller listing window	display	Displays a list of available controllers that have been configured in the system.
OK	push button	Click this button to add the action and exit out of the ISC Database Download Properties window.
Cancel	push button	Click this button to exit the ISC Database Download Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

ISC Database Download Properties Window Procedures

Add an ISC Database Download Action

1. Display the ISC Database Download Properties window.
2. Select the **Max number of panels to be downloaded at a time**.
3. From the Access Panel listing window, click on an entry to select it.

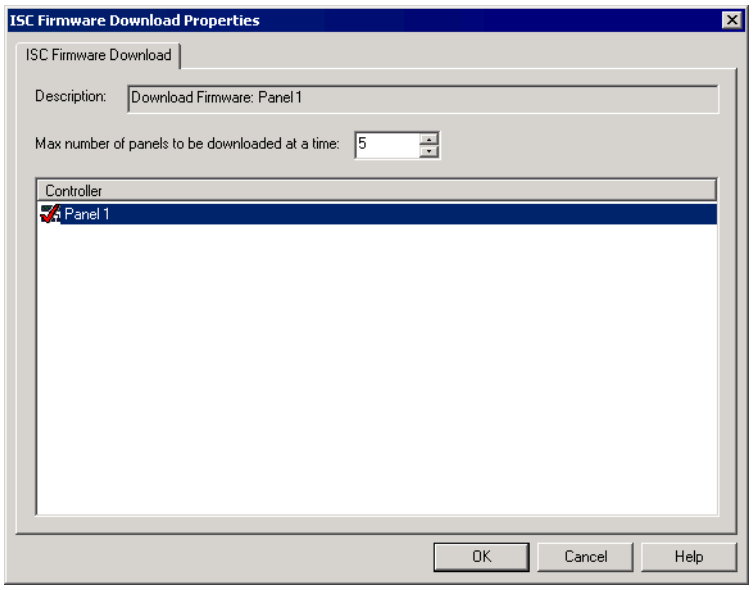
Note: You can select multiple entries.

4. Click [OK].

ISC Firmware Download Properties Window

Displayed by clicking [Add] on the Action Group Properties window and selecting **ISC Firmware Download** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.

You can also select the “Action Types”/ “ISC Firmware Download” **Category**/ **Object** combination in the **Add Action Wizard**.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

ISC Firmware Download Properties Window Field Table

Form Element	Type	Comment
Description	text	Displays a description of the access panel which is selected in the Access Panel listing window. **Note:** This field only displays a description when one and only one access panel is selected.
Max number of panels to be downloaded at a time	spin buttons	When configuring a firmware download as an action, select the maximum number of access panels that can be downloaded at a time.
Controller listing window	display	Displays a list of available controllers that have been configured in the system.
OK	push button	Click this button to add the action and exit out of the ISC Firmware Download Properties window.
Cancel	push button	Click this button to exit the ISC Firmware Download Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

ISC Firmware Download Properties Window Procedures

Add an ISC Firmware Download Action

1. Display the ISC Firmware Download Properties window.
2. Select the **Max number of panels to be downloaded at a time**.
3. From the Access Panel listing window, click on an entry to select it.

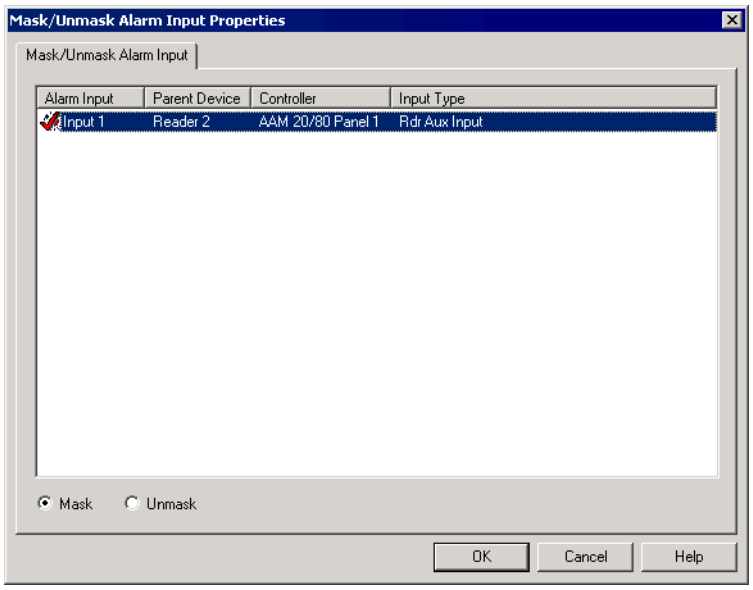
Note: You can select multiple entries.

4. Click [OK].

Mask/Unmask Alarm Input Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Alarm Input” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Alarm Input** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Alarm Input Properties Window Field Table

Form Element	Type	Comment
Alarm Input listing window	display	Displays a list of available alarm inputs which have been configured in the system.
Mask	radio button	When configuring a mask/unmask alarm input action, select this radio button if you want the alarm input to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask alarm input action, select this radio button if you want the alarm input to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Alarm Input Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Alarm Input Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Alarm Input Properties Window Procedures

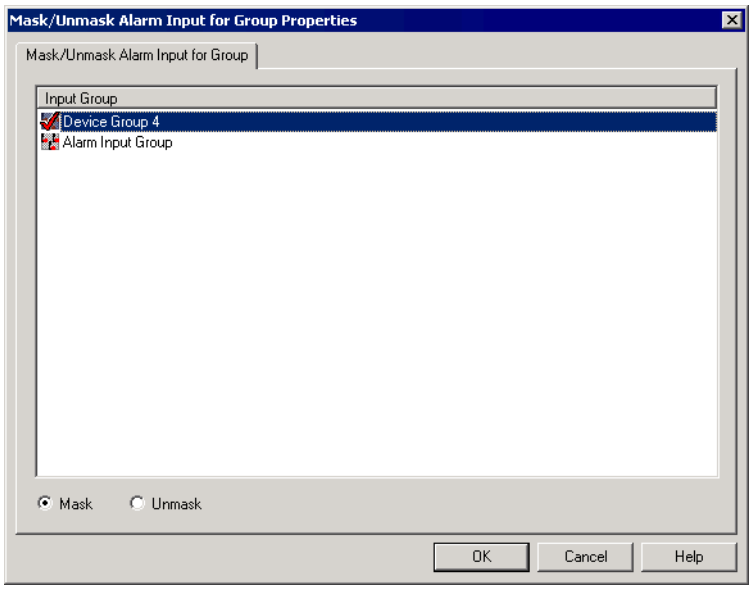
Add a Mask/Unmask Alarm Input Action

1. Display the Mask/Unmask Alarm Input Properties window.
2. From the Alarm Input listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want the alarm input to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the alarm input to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Alarm Input for Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Alarm Input for Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Alarm Input for Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Alarm Input for Group Properties Window Field Table

Form Element	Type	Comment
Input Group listing window	display	Displays a list of available alarm input groups which have been configured in the system.
Mask	radio button	When configuring a mask/unmask alarm input for group action, select this radio button if you want the group of alarm inputs to be masked. When alarm input groups are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask alarm input for group action, select this radio button if you want the group of alarm inputs to be unmasked. When alarm input groups are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Alarm Input for Group Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Alarm Input for Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Alarm Input for Group Properties Window Procedures

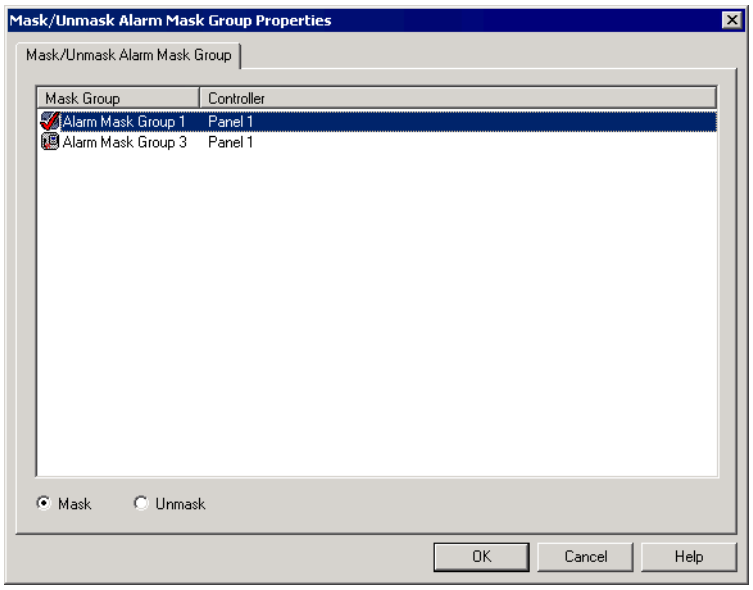
Add a Mask/Unmask Alarm Input For Group Action

1. Display the Mask/Unmask Alarm Input for Group Properties window.
2. From the Input Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want the alarm inputs in the group to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the alarm inputs in the group to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Alarm Mask Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Alarm Mask Group” **Category**/ **Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Alarm Mask Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Alarm Mask Group Properties Window Field Table

Form Element	Type	Comment
Mask Group listing window	display	Displays a list of available alarm mask groups which have been configured in the system.
Mask	radio button	When configuring a mask/unmask alarm mask group action, select this radio button if you want the mask group to be masked. When alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask alarm mask group action, select this radio button if you want the mask group to be unmasked. When alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Alarm Mask Group Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Alarm Mask Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Alarm Mask Group Properties Window Procedures

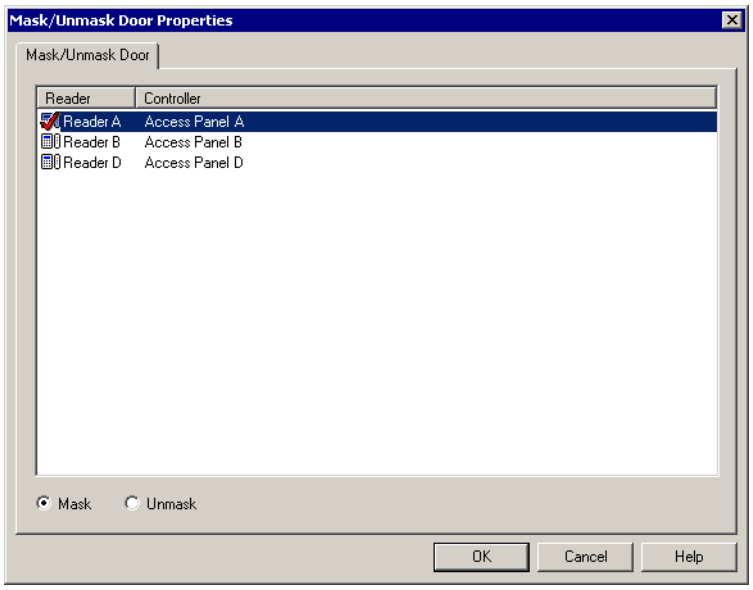
Add a Mask/Unmask Alarm Mask Group Action

1. Display the Mask/Unmask Alarm Mask Group Properties window.
2. From the Mask Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want the mask group to be masked. When alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the mask group to be unmasked. When alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Door” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Door** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Form Properties Window Table

Form Element	Type	Comment
Reader/Controller listing window	display	Displays a list of readers that are available for selection and the controllers that are associated with each.
Mask	radio button	When configuring a mask/unmask door action, select this radio button if you want the action to be that the door is masked. When masked doors generate alarms, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask door action, select this radio button if you want the action to be that the door is unmasked. When unmasked doors generate alarms, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Door Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Door Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Door Properties Window Procedures

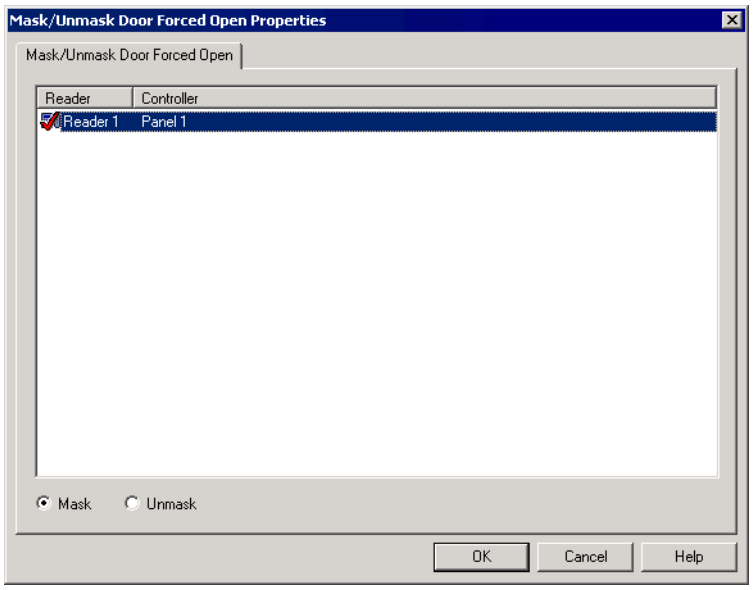
Add a Mask/Unmask Door Action

1. Display the Mask/Unmask Door Properties window.
2. From the Reader/Controller listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want the action to be that the door is masked. When masked doors generate alarms, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the action to be that the door is unmasked. When unmasked doors generate alarms, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Forced Open Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Door Forced Open” **Category**/ **Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Door Forced Open** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Forced Open Properties Window Field Table

Form Element	Type	Comment
Reader/Controller listing window	display	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
Mask	radio button	When configuring a mask/unmask door forced open action, select this radio button if you want the door forced open alarm to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask door forced open action, select this radio button if you want the door forced open alarm to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Door Forced Open Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Door Forced Open Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Door Forced Open Properties Window Procedures

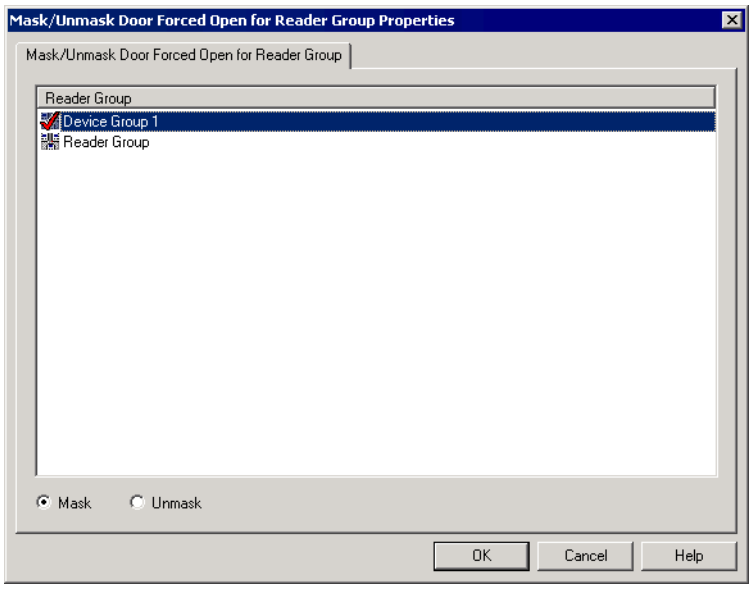
Add a Mask/Unmask Door Forced Open Action

1. Display the Mask/Unmask Door Forced Open Properties window.
2. From the Reader/Controller listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want door forced open alarms for the selected reader to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door forced open alarms for the selected reader to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Forced Open for Reader Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Door Forced Open for Reader Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Door Forced Open for Reader Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Forced Open for Reader Group Field Table

Form Element	Type	Comment
Reader Group listing window	display	Displays a list of available reader groups which have been configured in the system.
Mask	radio button	When configuring a mask/unmask door forced open for reader group action, select this radio button if you want the door forced open alarms to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask door forced open for reader group action, select this radio button if you want the door forced open alarms to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Door Forced Open for Reader Group Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Door Forced Open for Reader Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Door Forced Open for Reader Group Properties Window Procedures

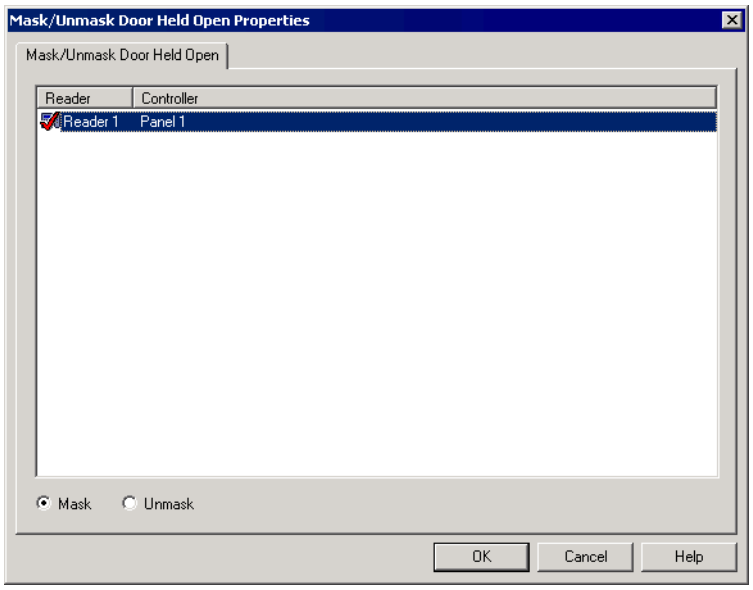
Add a Mask/Unmask Door Forced Open for Reader Group Action

1. Display the Mask/Unmask Door Forced Open for Reader Group Properties window.
2. From the Reader Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want door forced open alarms for the selected reader group to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door forced open alarms for the selected reader group to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Held Open Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Door Held Open” **Category**/ **Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Door Held Open** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Held Open Properties Window Field Table

Form Element	Type	Comment
Reader/Controller listing window	display	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
Mask	radio button	When configuring a mask/unmask door held open action, select this radio button if you want the door held open alarm to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask door held open action, select this radio button if you want the door held open alarm to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Door Held Open Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Door Held Open Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Door Held Open Properties Window Procedures

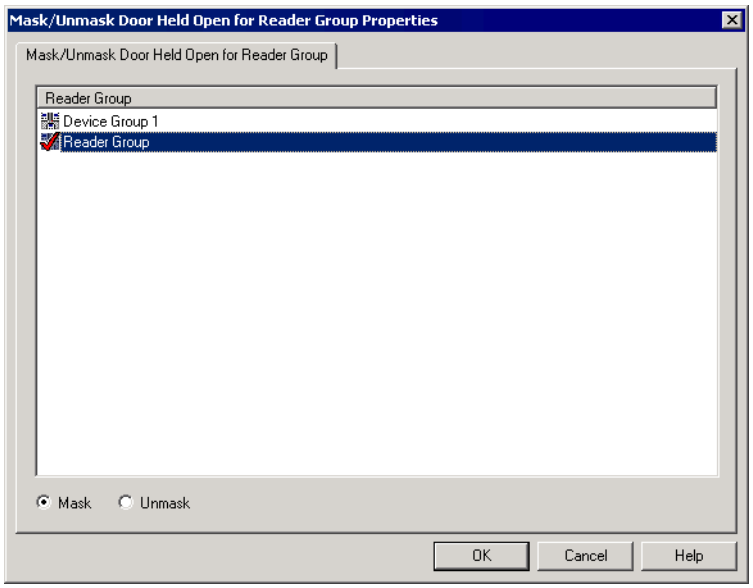
Add a Mask/Unmask Door Held Open Action

1. Display the Mask/Unmask Door Held Open Properties window.
2. From the Reader/Controller listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want door held open alarms for the selected reader to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door held open alarms for the selected reader to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Held Open for Reader Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Mask/Unmask Door Held Open for Reader Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Mask/Unmask Door Held Open for Reader Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Held Open for Reader Group Field Table

Form Element	Type	Comment
Reader Group listing window	display	Displays a list of available reader groups which have been configured in the system.
Mask	radio button	When configuring a mask/unmask door held open for reader group action, select this radio button if you want the door held open alarms to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	radio button	When configuring a mask/unmask door held open for reader group action, select this radio button if you want the door held open alarms to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	push button	Click this button to add the action and exit out of the Mask/Unmask Door Held Open for Reader Group Properties window.
Cancel	push button	Click this button to exit the Mask/Unmask Door Held Open for Reader Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Mask/Unmask Door Held Open for Reader Group Properties Window Procedures

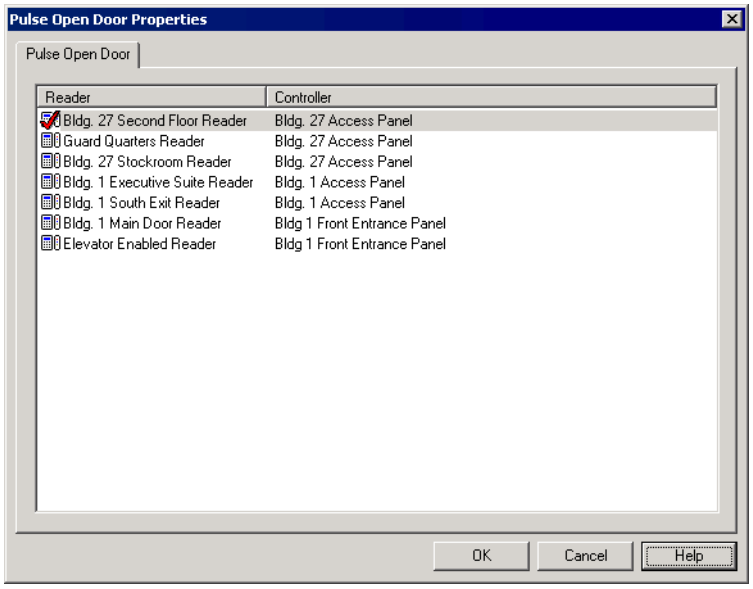
Add a Mask/Unmask Door Held Open for Reader Group Action

1. Display the Mask/Unmask Door Held Open for Reader Group Properties window.
2. From the Reader Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want door held open alarms for the selected reader group to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door held open alarms for the selected reader group to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Pulse Open Door Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Pulse Open Door” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Pulse Open Door** form the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Pulse Open Door Properties Window Field Table

Form Element	Type	Comment
Reader/controller listing window	display	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
OK	push button	Click this button to add the action and exit out of the Pulse Open Door Properties window.
Cancel	push button	Click this button to exit the Pulse Open Door Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Pulse Open Door Properties Window Procedures

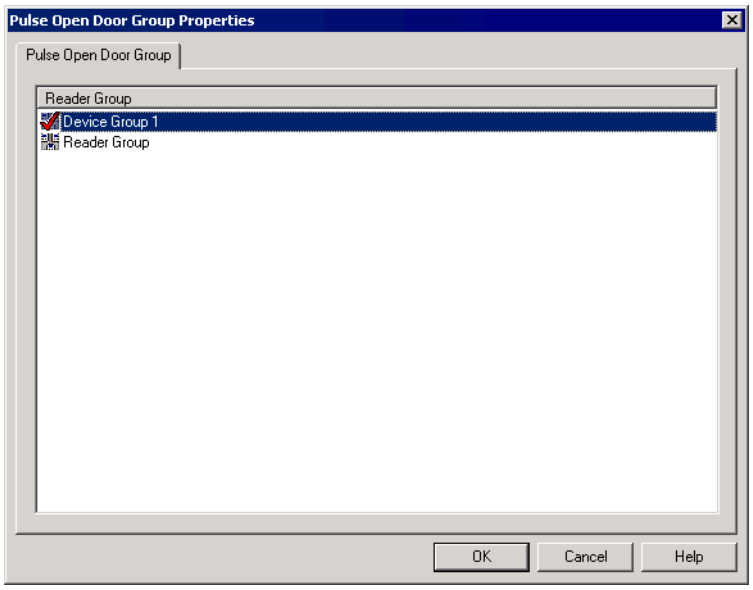
Add a Pulse Open Door Action

1. Display the Pulse Open Door Properties window.
2. From the listing window, click on an entry to select it.
3. Click [OK]. The pulse open door action (the door opens and then closes) is now configured for the selected reader.

Pulse Open Door Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Pulse Open Door Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Pulse Open Door Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Pulse Open Door Group Properties Window Field Table

Form Element	Type	Comment
Reader Group listing window	display	Displays a list of available readers groups which have been configured in the system.
OK	push button	Click this button to add the action and exit out of the Pulse Open Door Group Properties window.
Cancel	push button	Click this button to exit the Pulse Open Door Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Pulse Open Door Group Properties Window Procedures

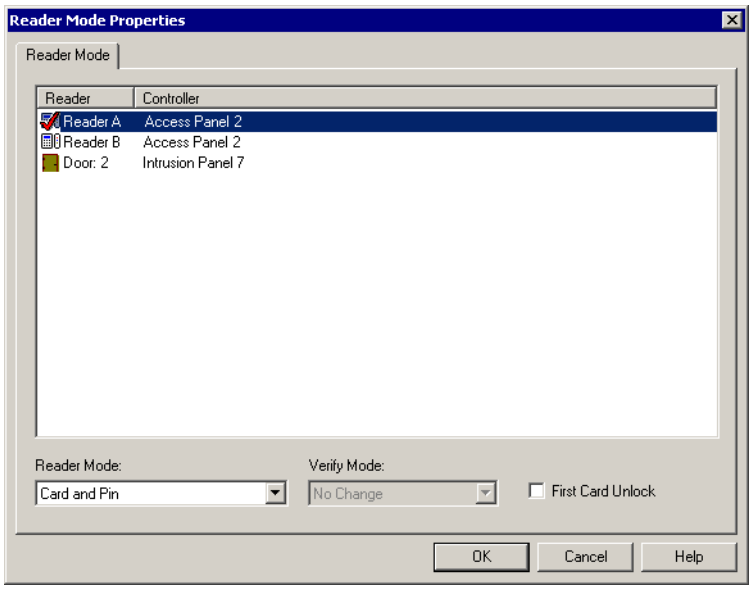
Add a Pulse Open Door Group Action

1. Display the Pulse Open Door Group Properties window.
2. From the Reader Group listing window, click on an entry to select it.
3. Click [OK]. The pulse open door group action (the doors open and then close) is now configured for the selected reader.

Reader Mode Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Reader Mode” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Reader Mode** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Reader Mode Form Properties Window Table

Form Element	Type	Comment
Reader/Controller listing window	display	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
Reader Mode	drop-down list	When configuring a reader mode action, select a mode from this drop-down list. Choices include: • Card Only • Facility Code Only • Locked • Card AND Pin • Pin OR Card • Unlocked
Verify Mode	drop-down list	When configuring a reader mode action for a reader on a Best controller that is a primary reader to an alternate biometric reader, you can select a verify mode. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader. When configuring a reader mode action for a reader that is not a primary reader to an alternate biometric reader, this field is disabled.
First Card Unlock	checkbox	Select this checkbox if you want the reader mode action to be that first card unlock mode is enabled. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.
OK	push button	Click this button to add the action and exit out of the Reader Mode Properties window.
Cancel	push button	Click this button to exit the Reader Mode Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Reader Mode Properties Window Procedures

Add a Reader Mode Action

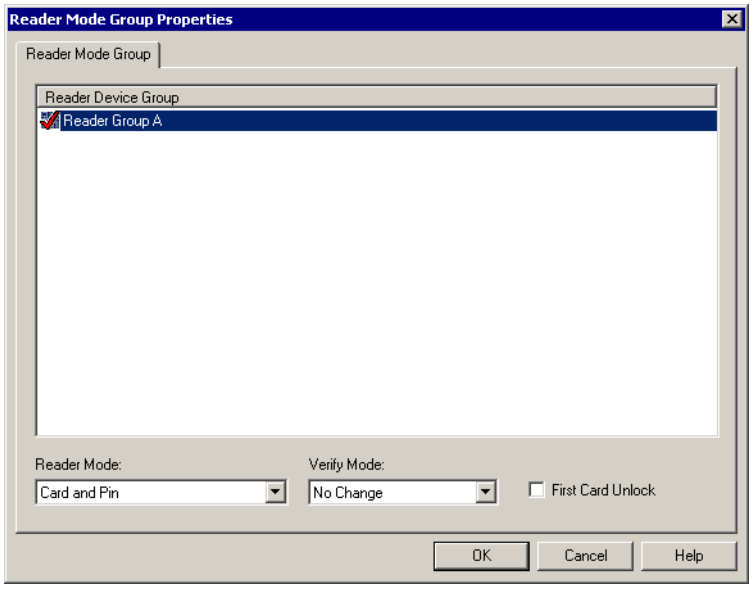
1. Display the Reader Mode Properties window.

2. From the Reader/Controller listing window, click on an entry to select it.
3. From the **Reader Mode** drop-down list, select a reader mode for the selected reader/controller.
4. When configuring a reader mode action for a reader on a Best controller that is a primary reader to an alternate biometric reader, you can select a **Verify Mode**. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader.
5. Select the **First Card Unlock** checkbox if you want this reader mode action to enable first card unlock.
6. Click [OK].

Reader Mode Group Properties Window

To display, do one of the following:

- Select the “Action Types”/ “Reader Mode Group” **Category**/**Object** combination in the **Add Action Wizard**.
- Click the [Add] button on the Action Group Properties window and then select **Reader Mode Group** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Reader Mode Group Properties Window Field Table

Form Element	Type	Comment
Reader Device Group listing window	display	Displays a list of available reader groups which have been configured in the system.
Reader Mode	drop-down list	When configuring a reader mode group action, select a mode from this drop-down list. Choices include: • Card Only • Facility Code Only • Locked • Card AND Pin • Pin OR Card • Unlocked
Verify Mode	drop-down list	When configuring a reader mode group action for a group of readers on a Best controller that are primary readers to alternate biometric readers, you can select a verify mode. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader. When configuring a reader mode group action for readers that are not primary readers alternate biometric readers, this field is disabled.
First Card Unlock	checkbox	Select this checkbox if you want the reader mode group action to be that first card unlock mode is enabled. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time.
OK	push button	Click this button to add the action and exit out of the Reader Mode Group Properties window.
Cancel	push button	Click this button to exit the Reader Mode Group Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Reader Mode Group Properties Window Procedures

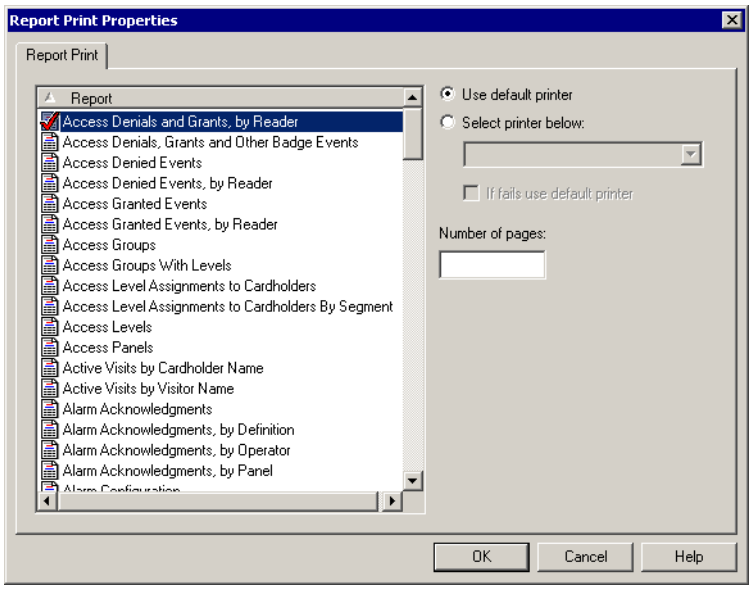
Add a Reader Mode Group Action

1. Display the Reader Mode Group Properties window.
2. From the Reader Device Group listing window, click on an entry to select it.
3. From the **Reader Mode** drop-down list, select a reader mode for the selected reader group.
4. When configuring a reader mode group action for readers on a Best controller that are primary readers to alternate biometric readers, you can select a **Verify Mode**. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader.
5. Select the **First Card Unlock** checkbox if you want this reader mode group action to enable first card unlock.
6. Click [OK].

Report Print Properties Window

Displayed by clicking [Add] on the Action Group Properties window and selecting **Report Print** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.

You can also select the “Action Types”/ “ISC Database Download” **Category**/ **Object** combination in the **Add Action Wizard**.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Report Print Properties Window Field Table

Form Element	Type	Comment
Report listing window	display	Displays a list of available reports.
Use default printer	radio button	Select this radio button if you want the scheduled report to print from the workstation's default printer.
Select printer below	radio button/drop-down list	Select this radio button and choose a printer from the drop-down list if you want the scheduled report to print to a printer other than the workstation's default printer. **Note:** The choices in the drop-down list are printers that are available for the workstation running the linkage server and not for the workstation that the action is being configured on.
If fails use default printer	checkbox	If you selected the **Select printer below** radio button, select this checkbox if you want to print from the default printer if the selected printer does not exist. **Note:** Due to a limitation of Crystal Reports this setting is not enforced if the printer exists but is not accessible under the linkage server account. When this occurs the report will automatically be printed from the default printer regardless of this setting.
Number of pages	numeric	When configuring a report print action, you can enter the number of pages that you want the report to have.
OK	push button	Click this button to add the action and exit out of the Report Print Properties window.
Cancel	push button	Click this button to exit the Report Print Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Report Print Properties Window Procedures

Add a Report Print Action

1. Display the Report Print Properties window.
2. From the Report listing window, click on an entry to select it.
3. Do one of the following:
   a. Select the **Use default printer** radio button if you want the scheduled report to print from the workstation's default printer.
   b. Select the **Select printer below** radio button and choose a printer from the drop-down list if you want the scheduled report to print to a printer other than the workstation's default printer.

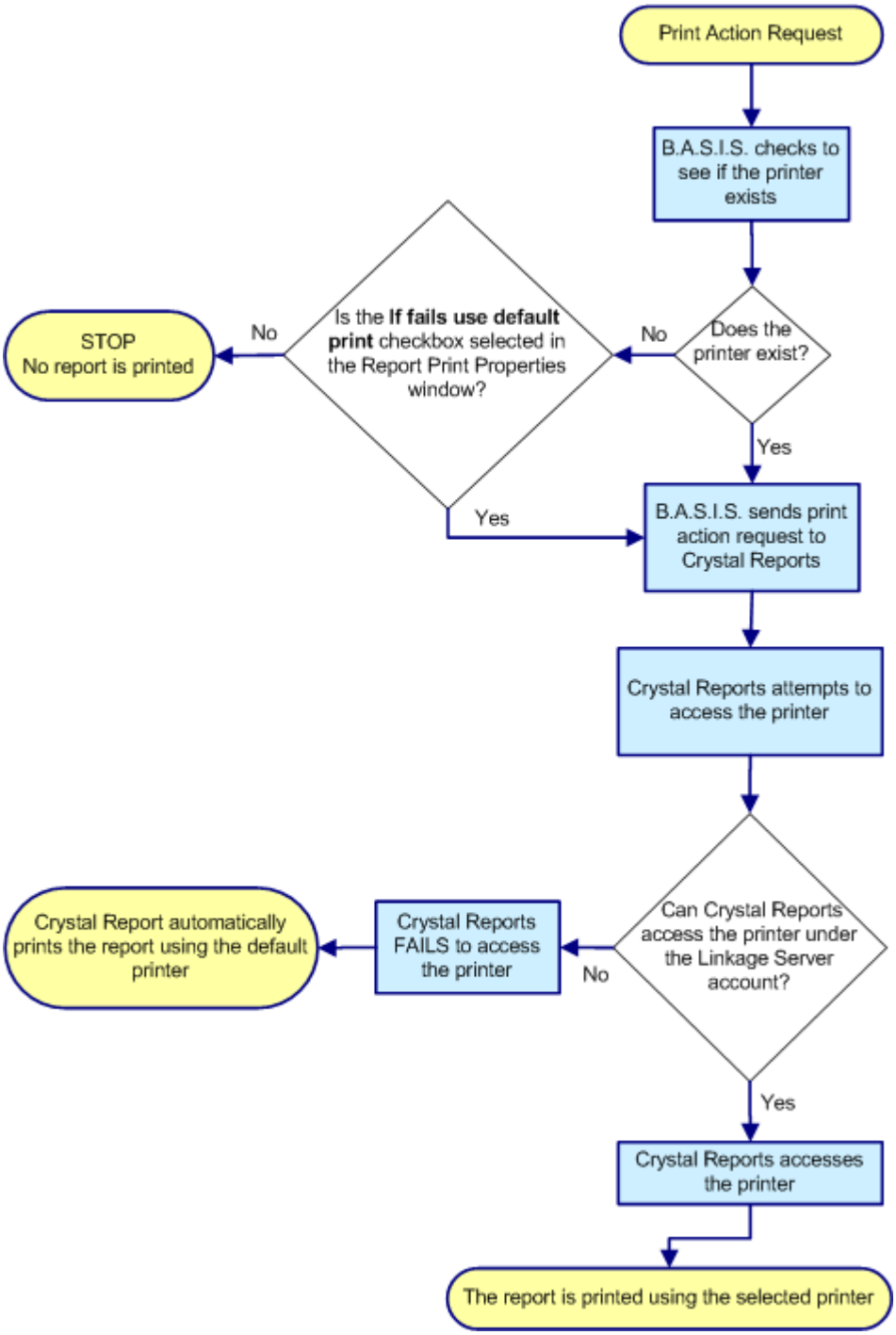
Note: If the linkage server is running under a local system account it may not have permission to access a network printer (depending on its configuration). If this is the case you must select a local or default network printer. Contact your System Administrator to determine what account the linkage server is running under and the printers it can access.

4. If you selected the **Select printer below** radio button, select the **If fails use default printer** checkbox if you want to print from the default printer if the selected printer fails.

Note: Due to a limitation of Crystal Reports, this setting is not enforced if the printer exists but is not accessible under the linkage server account. If the Crystal Report engine fails to access the printer it automatically prints to the default printer regardless of whether the **If fails use default printer** checkbox is selected or not. Refer to the report print action request flowchart below for different scenarios.

5. In the **Number of pages** field, enter the number of pages that you want the report to have.
6. Click [OK].

Request Print Action Flowchart

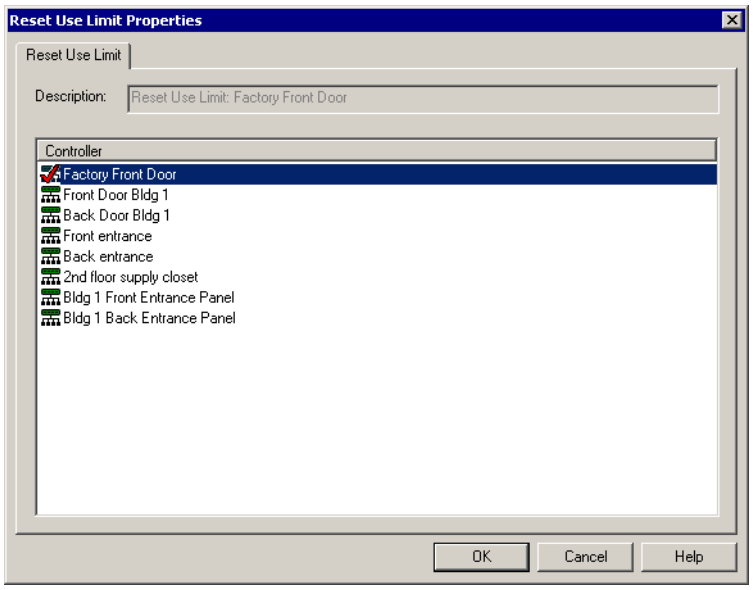

Print Action Request
B.A.S.I.S. checks to see if the printer exists
Does the printer exist?
No
Is the **If fails use default print** checkbox selected in the Report Print Properties window?
No
STOP
No report is printed
Yes
Yes
B.A.S.I.S. sends print action request to Crystal Reports
Crystal Reports attempts to access the printer
Can Crystal Reports access the printer under the Linkage Server account?
No
Crystal Reports FAILS to access the printer
Crystal Report automatically prints the report using the default printer
Yes
Crystal Reports accesses the printer
The report is printed using the selected printer

This flowchart shows how a report may get printed from the default printer although the **If fails use default printer** checkbox is NOT selected in the Report Print Properties window.

Reset Use Limit Properties Window

Displayed by clicking [Add] on the Action Group Properties window and selecting **Reset Use Limit** from the Select Action Type window. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.

You can also select the “Action Types”/ “ISC Database Download” **Category**/ **Object** combination in the **Add Action Wizard**.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Reset Use Limit Form Properties Window Table

Form Element	Type	Comment
Description	text	When one controller is selected in the listing window, displays the text "Reset Use Limit:" followed by the controller name. For example, "Reset Use Limit: Front Door Bldg 1." When more than one controller is selected in the listing window, this field is activated. Type in a descriptive name to identify the selected group of controllers.
Controller listing window	display	Displays a list of available controllers.
OK	push button	Click this button to add the reset use limit action for the selected controller(s) and exit out of the Reset Use Limit Properties window. **Note:** Each time a use-limited badge is used at a reader, the badge's use limit is decremented for the associated controller. A cardholder's use limit is specified on the Badge form of the Cardholders folder. Whenever the cardholder swipes their badge at a reader where use limits are enforced, the cardholder's use limit is reduced by one (1). When the use count reaches zero (0), the cardholder is unable to access use limit-enforced card readers on that controller.
Cancel	push button	Click this button to exit the Reset Use Limit Properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Reset Use Limit Properties Window Procedures

Add a Reset Use Limit Action

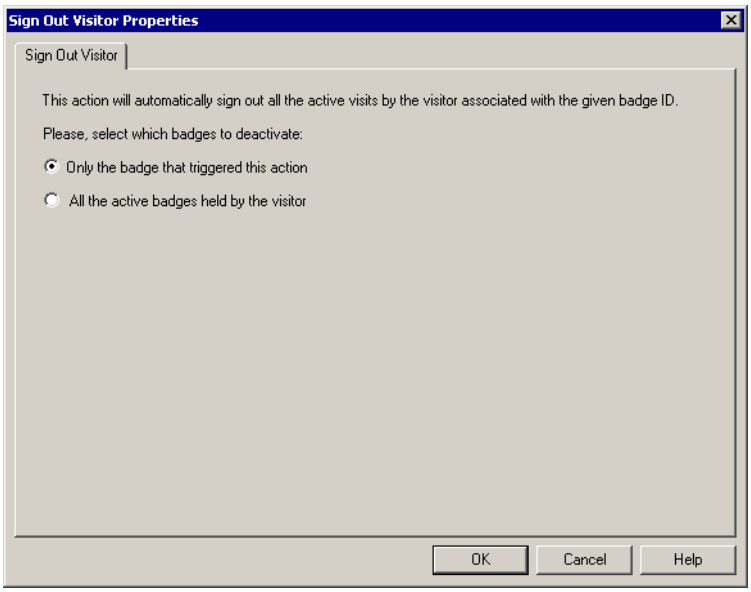
1. Display the Reset Use Limit Properties window.
2. Select one or more controller from the listing window.
3. If you selected one controller from the listing window, skip this step. If you selected more than one controller from the listing window, type a descriptive name to identify the selected group of controllers in the **Description** field.
4. Click [OK].

Sign Out Visitor Properties Window

The Sign Out Visitor action allows you to deactivate the badges of cardholders who have signed out of the system. You can further modify this action by choosing which of the cardholder's badges will be signed out, just the badge that triggered the action or all badges belonging to that cardholder.

To display, do one of the following:

- Clicking [Add] on the Output Action tab in the Global I/O form.
- An Action of this type can only be utilized from the Global I/O. In order to execute the action, Global I/O should have a linkage configured on a device, event, and badge ID that is passed to the action at runtime.


Sign Out Visitor Properties
Sign Out Visitor
This action will automatically sign out all the active visits by the visitor associated with the given badge ID.
Please, select which badges to deactivate:
Only the badge that triggered this action
All the active badges held by the visitor
OK
Cancel
Help

Sign Out Visitor Properties Properties Window Field Table

Form Element	Type	Comment
Only the badge that triggered this action	radio button	Select if you want to deactivate only the badge that caused the visitor to sign out.
All the active badges held by the visitor	radio button	Select if you want all the badges belonging to the visitor to deactivate once the visitor is signed out.
OK	push button	Click this button to add the action and exit out of the Sign Out Visitor properties window.
Cancel	push button	Click this button to exit the Sign Out Visitor properties window without adding the action.
Help	push button	Click this button to display online help for this window.

Sign Out Visitor Properties Window Procedures

Add a Sign Out Visitor Action

1. From the **Access Control** menu, select Global I/O.
2. Click [Add] on the Output Action sub tab of the Global Linkage form. The Add Action Wizard window opens.
3. Click Sign Out Visitor on the Objects area.
4. Click [Next]. The Sign Out Visitor Properties window appears.
5. Choose the options that suit your needs.
6. Click [OK].

Appendix B: Alarm/Event Descriptions

Alarm	Event	Event Type	Description
Accepted Biometric Score	Accepted Biometric Score	Biometric	This event returns the accepted biometric score. The actual access granted event is sent separately. This event is mainly used for diagnostic purposes.
Access Denied: Biometric Reader Offline	Access Denied: Biometric Reader Offline	Access Denied	Generated when the alternate biometric reader could not be contacted for verification (was offline).
Access Denied: No Biometric Template	Access Denied: No Biometric Template	Access Denied	Generated when the cardholder did not have a biometric template loaded in the database, so a verification could not be done.
Access Denied: Reader Locked	Access Denied: Reader Locked	Access Denied	Generated when access was denied because the reader was locked.
Access Granted: Reader Unlocked	Access Granted: Reader Unlocked	Access Granted	Generated when access was granted because the reader was unlocked.
Acknowledgment Action Executed	Acknowledgment Action Executed	System	Generated when an alarm is acknowledged and actions associated with the alarm are executed.
Acknowledgment Action Failed	Acknowledgment Action Failed	System	Generated when there is a failure to execute actions associated with an alarm acknowledgment.
Alarm Active	Alarm Active	System	Generated when an alarm has become active.
Alarm Monitoring Action Group Executed	Alarm Monitoring Action Group Executed	System	Generated when the action group is executed.
Alarm Monitoring Action Group Failed	Alarm Monitoring Action Group Failed	System	Generated when the action group execution fails.
Alarm Restored	Alarm Cancelled	System	Generated when a device has come online or an alarm condition has been restored.
All Systems Normal	All Systems Normal	Fire	Generated when the Notifier AM-2020 panel is booted up. This alarm may also be sent when all existing alarm conditions are resolved.
Anti-Passback Violation	Anti-Passback Violation	Area APB	Generated when the cardholder was denied access because the entry would have violated the anti-passback rules for the area.

Alarm	Event	Event Type	Description
Archive Server Failure	Archive Server Failure	Video	Generic error indicating a failure on the archive server. This error indicates that the archive server could not move any more data from the video recorders to the archive server. The user will have to go to the physical archive server computer and review the windows event logs, remote storage application and logs, B.A.S.I.S. log files in the B.A.S.I.S.\logs directory, and also follow general trouble shooting techniques as outlined in the archive server manual to determine the specific cause of the alarm.
Area Closed	Area Closed	Area APB	Generated when access was denied because the area being entered is closed.
Area Limit Exceeded	Area Limit Exceeded	Area APB	Generated when access was denied because the area limit would have been exceeded.
Asset Denied - Asset Disable Command Sent	Asset Denied - Asset Disable Command Sent	Asset	Generated when the asset was denied and the asset disable command was sent to disable the asset.
Asset Denied - Invalid Access	Asset Denied - Invalid Access	Asset	Generated when the asset was denied because the cardholder had invalid access levels.
Asset Denied - Invalid Asset	Asset Denied - Invalid Asset	Asset	Generated when the asset was denied because of an invalid asset (the asset was not found in the controller).
Asset Denied - Invalid Cardholder	Asset Denied - Invalid Cardholder	Asset	Generated when the asset was denied because of an invalid cardholder.
Asset Denied - No Asset Privileges	Asset Denied - No Asset Privileges	Asset	Generated when the asset was denied because the cardholder had no asset privileges.
Asset Granted - Asset Owner	Asset Granted - Asset Owner	Asset	Generated when the asset was granted because the cardholder was the asset owner.
Asset Granted - Asset Privileges Only	Asset Granted - Asset Privileges Only	Asset	Generated when the asset was granted because the cardholder had asset privileges.
Audibles Silenced	Audibles Silenced	Fire	Generated when all the alarm bells have been turned off on the controller.
Audibles Unsilenced	Audibles Unsilenced	Fire	Generated when all the alarm bells have been turned back on for the controller.
Biometric Mismatch	Biometric Mismatch	Access Denied	Generated when the cardholder has a biometric template and the alternate reader was utilized to capture a template to match, but the captured template did not match the stored template.
Biometric Verify Mode Disabled	Biometric Verify Mode Disabled	System	Generated when biometric verify mode is disabled.

Alarm	Event	Event Type	Description
Biometric Verify Mode Enabled	Biometric Verify Mode Enabled	System	Generated when biometric verify mode is enabled. When biometric verify mode is enabled, the primary reader requires biometric verification from the alternate (biometric) reader.
Blind Camera	Blind Camera	Video	
Blind Camera Restored	Blind Camera Restored	Video	
Block Acknowledge	Block Acknowledge	Fire	Generated when a block acknowledge command is sent. This command acknowledges any existing unacknowledged alarms in the system all at once.
Cabinet Tamper Active	Cabinet Tamper	System	Generated when a cabinet tamper condition has been detected.
Cabinet Tamper Restored	Cancelled Cabinet Tamper	System	Generated when a cabinet tamper condition has been restored.
Call disconnected	Call disconnected	Intercom	Generated when an intercom call has been disconnected.
Call Failed	Call Failed	Intercom	Generated when a phone call fails.
Call to a busy subscriber	Call to a busy subscriber	Intercom	Generated when an intercom call has been placed to a busy subscriber.
Call to an open subscriber	Call to an open subscriber	Intercom	Generated when an intercom call has been placed to an open subscriber.
Call to a private subscriber	Call to a private subscriber	Intercom	Generated when a call has been placed to a private subscriber.
Capture Source Mismatch	Capture Source Mismatch	Video	
Camera Motion Detected	Camera Motion Detected	Video	
Camera Motion Detected Restored	Camera Motion Detected Restored	Video	
Camera Tamper Active	Camera Tamper Active	Video	
Camera Tamper Restored	Camera Tamper Restored	Video	
Cancel Entire Sale	Cancel Entire Sale	POS	Generated when a transaction is used to indicate that an entire sale was cancelled.
Cash Amount Tendered	Cash Amount Tendered	POS	Generated when an event is used to indicate that a cash amount has been tendered
Cash or Safe Drop	Cash or Safe Drop	POS	Generated when a transaction indicating a cash or safe drop has occurred.
Change Due	Change Due	POS	Generated when a transaction indicating the change due has occurred.

Alarm	Event	Event Type	Description
Charge Account Tender	Charge Account Tender	POS	Generated when a charge account was used as tender.
Check Tender	Check Tender	POS	Generated when a check was used as tender.
Cipher Mode Disabled	Cipher Mode Disabled	System	Generated when cipher mode is disabled for a reader.
Cipher Mode Enabled	Cipher Mode Enabled	System	Generated when cipher mode is enabled for a reader. When this occurs card data can be entered via the keypad.
Clerk Name or Number	Clerk Name or Number	POS	A transaction that reports the clerk's name or number.
Command (#) Set From Reader	Command (#) Set From Reader	System	Generated when the reader keypad command "(#)" was executed.
Command Pin +10 Set From Reader	Command Pin +10 Set From Reader	System	Indicates the reader command "Pin +10" was executed.
Command Pin +20 Set From Reader	Command Pin +20 Set From Reader	System	Indicates the reader command "Pin +20" was executed.
Communication Initialization Failed	Communication Initialization Failed	System	Generated when the Communication Server fails to initialize communications. For example if you are using RS-232 and have hyperterminal running and using COM1 and then you start up the Communication Server and it needs to use COM1 to communicate to a panel, it will fail to open up the serial port and this event will be logged.
Communications Lost	Communications Lost	System	Generated when communications to the device have been lost.
Communications Lost - Primary Path	Primary Communication Path Lost	System	Generated when the primary path lost communication with the host.
Communications Lost - Secondary Path	Secondary Communication Path Lost	System	Generated when the secondary path loses communication with the host.
Communications Path Switched - Primary to Secondary	Communications Path Switched - Primary to Secondary	System	Generated when the communication path has been switched from the primary path to the secondary path.
Communications Path Switched Secondary to Primary	Communications Path Switched Secondary to Primary	System	Generated when the communication path has switched from the secondary path to the primary path.
Communications Restored	Communications Restored	System	Generated when communications to the device have been restored.
Communications Restored - Primary Path	Primary Communication Path Restored	System	Generated when the primary path restored communication with the host.

Alarm	Event	Event Type	Description
Communications Restored - Secondary Path	Secondary Communication Path Restored	System	Generated when the secondary path restored communication with the host.
Complimentary Tender	Complimentary Tender	POS	Generated when the tender was complimentary.
Controller Connection Mismatch	Controller Connection Mismatch	System	Associated text in the event indicates the details of the error.
Controller Encryption Error	Controller Encryption Error	System	Associated text in the event indicates the details of the error.
Credit Card Tendered	Credit Card Tendered	POS	Generated when a credit card was used as tender.
Current Time	Current Time	POS	An event that reports the current time.
Database Error Event Polling Stopped	Database Error Event Polling Stopped	System	Generated by the communication server when there is a problem writing events to the database. This event is not written to the database but is sent to Alarm Monitoring clients. Polling of the events from the various hardware devices is stopped until the events can be written to the database.
Database Error in Panel Download	Database Error in Panel Download	System	Generated by the communication server when the database cannot be opened at the start of a database download to a controller.
Debit, ATM, Check Card Tender	Debit, ATM, Check Card Tender	POS	Transaction that indicated that a debit, ATM, or check card was used as tender.
Denied Low Battery	Denied Low Battery	Access Denied	Generated when access is denied because the battery on the device is low.
Denied, No Command Authority	Denied, No Command Authority	Access Denied	Generated when a reader command function was denied because the user did not have the command authority to execute the function.
Denied - No Host Approval	Denied - No Host Approval	Access Denied	Generated when access was denied because the host did not grant approval. This can happen because the host response did not come back in a timely fashion or the controller is offline with the host.
Denied, PIN Only Request	Denied, PIN Only Request	Access Denied	Generated when access was denied for a pin only request (either an invalid pin code or pin support is not enabled for the panel).
Denied, Reader Excluded	Denied, Reader Excluded	Access Denied	Generated when access was denied because the reader exclusion list was violated. This happens when using precision access exclusion and the cardholder has access to the reader via an access level, but the precision access exclusion list has removed access.

Alarm	Event	Event Type	Description
Denied - Unauthorized Assets	Denied - Unauthorized Assets	Access Denied	Generated when access was denied because of unauthorized assets.
Denied Under Duress	Access Denied Under Duress	Duress	Generated when the cardholder was denied access under duress.
Denied Unmask, Active Zones in Group	Denied Unmask - Active Zones in Group	Access Denied	Generated when the unmask command failed because there are still active zones in the group.
Deny Count Exceeded	Deny Count Exceeded	Access Denied	Generated when a specified number of invalid attempts are made in a row at a reader.
Deposit Amount Paid Pending Purchase	Deposit Amount Paid Pending Purchase	POS	Event indicating that a deposit amount paid pending purchase has occurred.
Deposit Return	Deposit Return	POS	Transaction for a deposit return.
Detector Test	Detector Test	Fire	Generated when the fire detection test is initiated.
Detector Test Fail	Detector Test Fail	Fire	Generated when the fire detection test fails.
Detector Test OK	Detector Test OK	Fire	Generated when the fire detection test is successfully completed.
Device Type Mismatch	Device Type Mismatch	System	Generated when the device is of a different type than what it has been configured for.
Dialup Last Connection Time Expired	Dialup Last Connection Time Expired	System	Generated by the communication server for dialup panels that have exceeded the set number of hours since their last connection. When this event is generated, the communication server will attempt to connect to the panel. If the dialup panel repeatedly receives this event, the panel should be investigated to see why it is not calling back.
Dialup Stored Command Limit Exceeded	Dialup Stored Command Limit Exceeded	System	Generated by the communication server for dialup panels that have exceeded their stored command limit. When this event is generated, the communication server will attempt to connect to the panel. If the dialup panel repeatedly receives this event, the panel should be investigated to see why it is not calling back.
Directional Motion Detected	Directional Motion Detected	Video	
Directional Motion Restored	Directional Motion Restored	Video	
Discount Entered as Absolute Amount	Discount Entered as Absolute Amount	POS	Generated when a discount was entered as an absolute amount.
Discount Entered as Percentage	Discount Entered as Percentage	POS	Generated when a discount was entered as a percentage.

Alarm	Event	Event Type	Description
Door Contact Tamper Active	Door Contact Tamper	System	Generated when the door contact tamper has gone active.
Door Contact Tamper Restored	Door Contact Tamper Cancelled	System	Generated when the door contact tamper has been restored.
Door Forced Open	Door Forced Open	System	Generated when a “Door Forced Open” condition has been detected.
Door Forced Open Masked	Door Forced Open Masked	System	Generated when the “Door Forced Open” event has become masked for the device.
Door Forced Open Restored	Door Forced Open Cancelled	System	Generated when a “Door Forced Open” condition has been restored.
Door Forced Open Unmasked	Door Forced Open Unmasked	System	Generated when the “Door Forced Open” event has become unmasked for the device.
Door Held Open	Door Held Open	System	Generated when a “Door Held Open” condition has been detected.
Door Held Open Masked	Door Held Open Masked	System	Generated when the “Door Held Open” event has become masked for the device.
Door Held Open Restored	Door Held Open Cancelled	System	Generated when a “Door Held Open” condition was restored.
Door Held Open Unmasked	Door Held Open Unmasked	System	Generated when the “Door Held Open” event has become unmasked for the device.
Door Shunt Command Executed From Reader	Door Shunt Command Executed From Reader	System	Generated when the door shunt command was executed from the reader.
Door Shunt Command Results - Cancelled	Door Shunt Command Results - Cancelled	System	Generated when the door is closed while the door shunt command is executing.
Driver Error in Panel Download	Driver Error in Panel Download	System	Generated by the communication server when an error occurs during a database download to a controller.
Employee Sign Off	Employee Sign Off	POS	Generated when an employee signs on.
Employee Sign On	Employee Sign On	POS	Generated when an employee signs off.
Extended Held Command Denied	Extended Held Command Denied	System	Generated when an extended held command is denied.
Extended Held Command Set From Reader	Extended Held Command Set From Reader	System	Generated when an extended held command is entered at a reader.
Extended Held Open Mode Disabled	Extended Held Open Mode Disabled	System	Generated when extended held open mode is disabled.
Extended Held Open Mode Enabled	Extended Held Open Mode Enabled	System	Generated when extended held open mode is enabled.
Failed to Report Expected Event	Failed to Report Expected Event	System	Generated when a device that is supposed to report an event within a certain period of time fails to report an event during this time period.

Alarm	Event	Event Type	Description
Fire Alarm	Fire Alarm	Fire	Generated when a fire device is in alarm.
Fire Alarm Acknowledge	Fire Alarm Acknowledge	Fire	Generated when a fire alarm has been acknowledged.
Fire Alarm Acknowledged Clear	Fire Alarm Acknowledged Clear	Fire	Generated when a fire alarm has been acknowledged and cleared.
Fire Alarm Block Acknowledge	Fire Alarm Block Acknowledge	Fire	Generated when all fire alarms have been acknowledged at the fire panel.
Fire Alarm In	Fire Alarm In	Fire	Generated when a new fire alarm has been detected for the device.
Fire Alarm Out	Fire Alarm Out	Fire	Generated when a device with a previous fire alarm has returned to its normal state.
First Card Unlock Mode Disabled	First Card Unlock Mode Disabled	System	Generated when first card unlock mode is disabled for a door.
First Card Unlock Mode Enabled	First Card Unlock Mode Enabled	System	Generated when first card unlock mode is enabled for a door. Doors configured for first card unlock mode will not unlock until a user with first card unlock authority gains entry.
Foil Break Alarm	Foil Break Alarm	Trouble	Generated when a break in a foil circuit occurs. This is most commonly used to trigger an alarm when glass being protected with the foil circuit is broken.
Foil Break Restore	Foil Break Restore	Trouble	Generated when a foil break alarm condition has been restored.
Foodstamps Tender	Foodstamps Tender	POS	Indicates that food stamps were used as tender.
Gasoline Prepayment	Gasoline Prepayment	POS	Transaction for a gasoline prepayment
Gasoline Prepayment Refund	Gasoline Prepayment Refund	POS	Transaction for a gasoline prepayment
Global Linkage Action Executed	Global Linkage Action Executed	System	Generated when a global I/O linkage has executed.
Global Linkage Action Failed	Global Linkage Action Failed	System	Generated when a global I/O linkage has failed.
Granted Access	Access Granted	Access Granted	Generated when access was granted.
Granted APB Violation, Entry Made	Access Granted Anti-Passback Used	Area APB	Generated when an anti-passback violation occurred but access was granted and entry was made. This can happen when using soft anti-passback.
Granted APB Violation, No Entry Made	Access Granted Anti-Passback Not Used	Area APB	Generated when an anti-passback violation occurred and access was granted but no entry was made. This can happen when using soft anti-passback.

Alarm	Event	Event Type	Description
Granted Facility Code	Access Granted On Facility Code	Access Granted	Generated when access was granted based on a valid facility code.
Granted Facility Code, No Entry	Access Granted On Facility Code No Entry Made	Access Granted	Generated when access was granted on facility code but no entry was made at the door.
Granted No Entry	Access Granted No Entry Made	Access Granted	Generated when access was granted but no entry was made at the door.
Granted Under Duress	Access Granted Under Duress	Duress	Generated when the cardholder was granted access under duress.
Granted Under Duress, No Entry	Access Granted Under Duress - No Entry Made	Duress	Generated when the cardholder was granted access under duress but no entry was made.
Grounded Loop Active	Grounded Loop Alarm Active	System	Generated when a grounded loop fault condition has been detected.
Grounded Loop Restored	Cancelled Grounded Loop	System	Generated when the grounded loop fault condition was restored.
Guard Tour Action Executed	Guard Tour Action Executed	System	Generated when a guard tour action has executed.
Guard Tour Action Failed	Guard Tour Action Failed	System	Generated when a guard tour action has failed.
Hold	Hold	Intercom	Generated when a phone call is placed on hold.
Host Executed Function List	Host Executed Function List	System	Generated when a function list has been executed from the host.
Inactive Badge	Inactive Badge	Access Denied	Generated when access was denied because the badge was inactive.
Incoming Call	Incoming Call	Intercom	Generated when there is an incoming call.
Information Message	Information Message	POS	Used to report information messages
Initiated	Initiated	Intercom	Generated when a phone call is initiated.
Input Alarmed	Input Alarmed	Generic	
Input High	Input High	Generic	
Input High High	Input High High	Generic	
Input Low	Input Low	Generic	
Input Low Low	Input Low Low	Generic	
Input Normal	Input Normal	Generic	
Input Masked	Input Masked	System	Generated when an input has become masked.
Input Unmasked	Input Unmasked	System	Generated when an input has become unmasked.

Alarm	Event	Event Type	Description
Intercom Function	Intercom Function	Intercom	Generated when an intercom function has been executed.
Invalid Access Level	Invalid Access Level	Access Denied	Generated when access was denied because of an invalid access level.
Invalid Badge	Invalid Badge	Access Denied	Generated when access was denied because the badge ID was unknown to the controller.
Invalid Card Format	Invalid Card Format	Access Denied	Generated when the badge contained a card format that was not recognized by the reader.
Invalid Device Serial Number	Invalid Device Serial Number	System	Generated when the device does not have a valid serial number.
Invalid Facility Code	Invalid Facility Code	Access Denied	Generated when access was denied because the badge had an invalid facility code.
Invalid Issue Code	Invalid Issue Code	Access Denied	Generated when access was denied because the issue code read from the badge did not match the current issue code stored in the database for the badge.
Invalid PIN	Invalid PIN Number	Access Denied	Generated when access was denied because an invalid PIN was entered.
Item Correct of Previously entered Item	Item Correct of Previously entered Item	POS	Generated to indicate that an item was corrected.
Item Sold	Item Sold	POS	Indicates an item was sold.
Key Override	Key Override	System	Generated when the key override is used in a Mortise lockset. Not supported in Cylindrical lockset.
Lamp Test Activated	Lamp Test Activated	Fire	Generated when the lamp test is activated. When a lamp test is activated the AM-2020 will send out a command sequence to display a set of solid blocks on the hardware's LCD.
Lamp Test Complete	Lamp Test Complete	Fire	Generated when the lamp test successfully completes.
Motion Detected	Motion Detected	Video	
Motion Detected Restored	Motion Detected Restored	Video	
Line Error Active	Line Error Active	System	Generated when a line error fault condition has been detected.
Line Error Restored	Cancelled Line Error	System	Generated when the line error fault condition was restored.
Local I/O Executed Function List	Local I/O Executed Function List	System	Generated when a local I/O function list has been activated.
Lottery Pay Out	Lottery Pay Out	POS	Generated when a lottery pay out has occurred.

Alarm	Event	Event Type	Description
Lottery Sale	Lottery Sale	POS	Generated when an event for a lottery sale has occurred.
Low Voltage	Low Voltage	System	Generated when a low voltage condition has been detected at the device.
Low Voltage Restored	Low Voltage Restored	System	Generated when a device resumes its proper voltage.
Manufacturer Coupon	Manufacturer Coupon	POS	Indicates a manufacturer coupons.
Manufacturer Coupon Redemption	Manufacturer Coupon Redemption	POS	Transaction generated for a manufacturer coupon redemption.
Max Assets Reached	Max Assets Reached	System	Generated during a download when the number of assets exceeds the maximum value configured for the controller. Only the maximum number of assets will be downloaded (all others will be ignored).
Max Biometric Templates Reached	Max Biometric Templates Reached	System	Generated during a download when the number of biometric templates exceeds the maximum value configured for the controller. Only the maximum number of templates will be downloaded (all others will be ignored).
Max Cardholders Reached	Max Cardholders Reached	System	Generated during a download when the number of cardholders exceeds the maximum value configured for the controller. Only the maximum number of cardholders will be downloaded (all others will be ignored).
Merchandise Returned	Merchandise Returned	POS	Generated when merchandise is returned.
Miscellaneous Tender	Miscellaneous Tender	POS	Generated when miscellaneous tender is used.
Module Active	Module Active	Fire	Generated when a monitor or control module connected to the system becomes active. The device label assigned to this device and the zone label assigned to the first zone programmed for this device will be included with the event.
Module Clear	Module Clear	Fire	Generated when a monitor or control module connected to the system is no longer active. The device label assigned to this device and the zone label assigned to the first zone programmed for this device will be included with the event.
Motion Detected	Motion Detected	Video	Generated when motion has been detected on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera.

Alarm	Event	Event Type	Description
Motion Detected Restored	Motion Detected Restored	Video	Generated when motion has been restored (is no longer detected) on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera.
Muster Mode Reset	Muster Mode Reset	Muster	Generated when muster mode is reset.
Muster Mode Start	Muster Mode Start	Muster	Generated when muster mode is started.
Negative Tax	Negative Tax	POS	Generated when negative tax is used.
Negative Total	Negative Total	POS	Generated when there is a negative total.
No Biometric Template Data	No Biometric Template Data	Biometric	Generated when no biometric template data was available from the biometric reader at the end of a verification sequence.
Not Configured	Not Configured	System	Generated when a device has not been configured or defined by the host.
No Sale	No Sale	POS	Transaction generated for a no sale.
Open Line Active	Open Line Active	System	Generated when an open line fault condition has been detected.
Open Line Restored	Cancelled Open Line	System	Generated when the open line fault condition was restored.
Override Preprogrammed Price	Override Preprogrammed Price	POS	Generated when the preprogrammed price is overridden.
Panel Download Completed	Full Panel Download Completed	System	Generated when a database download to the controller has completed.
Panel Download Started	Full Panel Download Started	System	Generated when a database download to the controller has started.
Panel Free Memory Low	Panel Free Memory Low	System	Generated when the free memory in the panel (controller) is below what is determined to be a safe value.
Panel ID Mismatch	Panel ID Mismatch	System	Generated when the panel (controller) has a different ID than what is in the database. This can happen if a new panel or replacement panel is placed out in the field. A download to the panel should correct the problem.
Panel Options Mismatch	Panel Options Mismatch	System	Generated when the options inside of the panel differ from what the panel is currently configured for in the database. This can happen if the panel options change and a download is not issued to the panel. To correct this situation, a download should be issued to the panel.
Panel Power Up Complete	Panel Power Up Complete	System	Generated when the panel power up is complete.

Alarm	Event	Event Type	Description
Panic Abort	Panic Abort	Trouble	Generated when a panic alarm has been manually aborted/canceled.
Panic Alarm	Panic Alarm	Trouble	Generated when emergency assistance has been manually requested.
Panic Alarm Restore	Panic Alarm Restore	Trouble	Generated when the panic alarm has been restored.
Pay Out	Pay Out	POS	Generated when a payout takes place.
Payment of Refund to Customer	Payment of Refund to Customer	POS	Generated when a payment or refund is given to a customer.
Payment Toward Charge Account Balance	Payment Toward Charge Account Balance	POS	Generated when a payment toward an account balance.
Pick Up	Pick Up	POS	Transaction indicating a pick up has occurred.
Power Failure Active	Power Failure	System	Generated when a power failure condition has been detected.
Power Failure Restored	Cancelled Power Failure	System	Generated when the power failure condition was restored.
Price Lookup	Price Lookup	POS	Generated when a price lookup has taken place.
Quantity or Weight	Quantity or Weight	POS	An event indicating a quantity or weight.
Reader Input Tamper Active	Reader Input Tamper	System	Generated when the reader input tamper has gone active.
Reader Input Tamper Restored	Reader Input Tamper Cancelled	System	Generated when the reader input tamper was restored.
Reader Low Battery	Reader Low Battery	System	Generated when a reader has a low battery.
Reader Low Battery Restored	Reader Low Battery Restored	System	Generated when a reader low battery condition has been restored.
Reader Mode Card and Pin	Reader Mode Card and Pin	System	Generated when the reader mode has changed to “Pin and Card” for the device.
Reader Mode Card Only	Reader Mode Card Only	System	Generated when the reader mode has changed to “Card Only.”
Reader Mode Facility Code	Reader Mode Facility Code	System	Generated when the reader mode has changed to “Facility Code Only.”
Reader Mode First Card Unlock	Reader Mode First Card Unlock	System	Generated when the reader mode has changed to “First Card Unlock.”
Reader Mode Locked	Reader Mode Locked	System	Generated when the reader mode has changed to “Locked.”
Reader Mode Pin or Card	Reader Mode Pin or Card	System	Generated when the reader mode has changed to “Pin or Card” for the device.

Alarm	Event	Event Type	Description
Reader Mode Unlocked	Reader Mode Unlocked	System	Generated when the reader mode has changed to “Unlocked.”
Reader Motor Stalled	Reader Motor Stalled	System	Generated when the motor stalls on a reader.
Reader Motor Stalled Restored	Reader Motor Stalled Restored	System	Generated when a motor stalled condition has been restored.
Reader Reset	Reader Reset	System	Generated when the firmware resets the reader. This can happen if the reader is brand new or in the case of a failed/ incomplete download. Internal conditions, such as a possible corrupt memory, can also cause the firmware to reset. In these cases, the firmware will rewrite its entire storage with default values, overwriting the downloaded values. When this happens, the user must reprogram the lockset.
Register X Report	Register X Report	POS	Indicates a X report was generated. X reports are financial, end of day, clerk, etc. reports.
Register Z Report	Register Z Report	POS	Indicates a Z report was generated. Z reports are the same as X reports, but resets totals to zero.
Rejected Biometric Score	Rejected Biometric Score	Biometric	This event returns the rejected biometric score (the actual denied event is sent separately).
Relay Contact Activated	Relay Contact Activated	System	Generated when a relay contact was activated.
Relay Contact Deactivated	Relay Contact Deactivated	System	Generated when a relay contact was deactivated.
Retrieved	Retrieved	Intercom	Generated when a phone call is retrieved/ answered.
Ringing	Ringing	Intercom	Generated when an intercom station/phone is ringing.
Sales Subtotal	Sales Subtotal	POS	A transaction that reports the sale subtotal
Scheduler Action Executed	Scheduler Action Executed	System	Generated when a scheduler action has executed.
Scheduler Action Failed	Scheduler Action Failed	System	Generated when a scheduler action has failed.
Security Alarm Acknowledge	Security Alarm Acknowledge	Fire	Generated when a security alarm has been acknowledged.
Security Alarm Block Acknowledge	Security Alarm Block Acknowledge	Fire	Generated when all security alarms have been acknowledged at the fire panel.
Security Alarm In	Security Alarm In	Fire	Generated when a new security alarm has been detected for the device.

Alarm	Event	Event Type	Description
Security Alarm Out	Security Alarm Out	Fire	Generated when a device with a previous security alarm has returned to its normal state.
Shorted Line Active	Shorted Line Alarm Active	System	Generated when a shorted line fault condition has been detected.
Short Line Restored	Canceled Shorted Line	System	Generated when a device with a shorted line fault condition has returned to its normal state.
Signal Silence	Signal Silence	Fire	Generated when the alarm signal on the hardware has been silenced.
Smart Card Authentication Failed	Smart Card Authentication Failed	System	Generated when a smart card authentication failed.
Status In	Status In	Fire	Generated when a status reporting device is active.
Status Out	Status Out	Fire	Generated when a status reporting device has returned to the inactive state.
Storage Failure	Storage Failure	Video	
Store Coupon	Store Coupon	POS	Indicates a store coupon.
Supervisory Acknowledge	Supervisory Acknowledge	Fire	Generated when a supervisory condition has been acknowledged.
Supervisory Block Acknowledge	Supervisory Block Acknowledge	Fire	Generated when all supervisory conditions have been acknowledged at the fire panel.
Supervisory In	Supervisory In	Fire	Generated when a new supervisory condition has been detected for the device.
Supervisory Out	Supervisory Out	Fire	Generated when a device with a previous supervisory condition has returned to its normal state.
System Reset	System Reset	System	Generated when the fire panel has been reset.
Tax Amount	Tax Amount	POS	Event that indicates the tax amount.
Taxable Subtotal	Taxable Subtotal	POS	Transaction that reports the taxable subtotal
Timeout Exceeded - No Second Card	Timeout Exceeded - No Second Card	Area APB	Generated when no second card was presented within the time limit for the area/ reader using two-man control.
Total Amount Due	Total Amount Due	POS	Transaction indicating the total amount due.
Transaction Number	Transaction Number	POS	Event Generated that indicates the transaction number of the sales transaction.
Transfer, Diagnostics	Transfer, Diagnostics	System	Generated when a user is connected to the device for diagnostic purposes.
Transfer, History	Transfer, History	System	Generated when a history data was transferred from the device to the parent device.

Alarm	Event	Event Type	Description
Transfer, PDA To Lock	Transfer, PDA To Lock	System	Generated when the device (lockset) is programmed/reprogrammed through a download from a PDA.
Transmitter Alarm	Transmitter Alarm	Transmitter	Generated when the button or input on a transmitter has been activated.
Transmitter Alarm Restored	Transmitter Alarm Restored	Transmitter	Generated when the transmitter alarm has been restored.
Transmitter Inactivity	Transmitter Inactivity	Transmitter	Transmitter has been inactive longer than the supervision interval
Transmitter Low Battery	Transmitter Low Battery	Transmitter	Transmitter low battery alarm
Transmitter Low Battery Restored	Transmitter Low Battery Restored	Transmitter	Generated when a transmitter low battery has been restored.
Transmitter Pre-Tilt	Transmitter Pre-Tilt	Transmitter	Generated when the transmitter is in the pre-tilt state.
Transmitter Pre-Tilt Restored	Transmitter Pre-Tilt Restored	Transmitter	Generated when the transmitter has returned to normal from the pre-tilt state.
Transmitter Pull Cord Alarm	Transmitter Pull Cord Alarm	Transmitter	Generated when the pull cord on a transmitter has been pulled and is in alarm.
Transmitter Pull Cord Restored	Transmitter Pull Cord Restored	Transmitter	Generated when the transmitter pull cord alarm has been restored.
Transmitter Tamper	Transmitter Tamper	Transmitter	Transmitter tamper alarm.
Transmitter Tamper Restored	Transmitter Tamper Restored	Transmitter	Generated when a transmitter tamper has been restored.
Transmitter Temporary Tilt Disable	Transmitter Temporary Tilt Disable	Transmitter	Generated when the transmitter temporary tilt has been disabled.
Transmitter Tilt	Transmitter Tilt	Transmitter	Generated when a tilt condition on the transmitter has been detected.
Transmitter Tilt Disabled	Transmitter Tilt Disabled	Transmitter	Generated when the transmitter tilt function has been disabled.
Transmitter Tilt Enabled	Transmitter Tilt Enabled	Transmitter	Generated when the transmitter tilt function has been enabled.
Transmitter Tilt Restored	Transmitter Tilt Restored	Transmitter	Generated when the tilt condition on the transmitter has been restored.
Trouble Acknowledge	Trouble Acknowledge	Fire	Generated when the trouble condition has been acknowledged.
Trouble Acknowledge Clear	Trouble Acknowledge Clear	Fire	Generated when a trouble condition that has been cleared from the system has been acknowledged by a user.
Trouble Bell #	Trouble Bell 1 or 2	Relay/ Sounder	Generated when trouble bell 1 or trouble bell 2 is in alarm.

Alarm	Event	Event Type	Description
Trouble Bell # Restore	Trouble Bell 1 or 2 Restore	Relay/ Sounder	Generated when trouble bell 1 alarm or trouble bell 2 alarm is restored.
Trouble Block Acknowledge	Trouble Block Acknowledge	Fire	Generated when all trouble conditions have been acknowledged at the fire panel.
Trouble In	Trouble In	Fire	Generated when a new trouble condition has been detected for the device.
Trouble Out	Trouble Out	Fire	Generated when a device with a previous trouble condition has returned to its normal state.
Trouble Report	Trouble Report	Intercom	Generated when there is trouble with a device. This event reports trouble and includes additional details in the associated text.
Unexpected Access	Unexpected Access	System	Generated when a user successfully exits using an unexpected exit reader, after gaining access to a specific entry reader, and the “must proceed to exit readers” option is enabled.
Unexpected Access Attempt	Unexpected Access Attempt	System	Generated when a user attempts to exit using an unexpected exit reader, after gaining access to a specific entry reader, and the “must proceed to exit readers” option is enabled.
Untyped Abort	Untyped Abort	Trouble	Generated when an alarm for a device of an unknown type has been aborted/canceled.
Untyped Alarm	Untyped Alarm	Trouble	Generated when an alarm for a device of unknown type occurs.
Untyped Alarm Restore	Untyped Alarm Restore	Trouble	Generated when the device of an unknown type is restored.
Untyped Bypass	Untyped Bypass	Trouble	Generated when a device of an unknown type has been bypassed.
Use Limit Exceeded	Use Limit Exceeded	Access Denied	Access was denied because the use limit for the badge has been exceeded.
User Failed to Reach Destination	User Failed to Reach Destination	System	Generated when a user fails to exit at a specific exit reader, after gaining access to a specific entry reader, before the timeout value expires.
User Generated Video Event	User Generated Video Event	Video	A user generated event can be created from any camera with any user-defined time limit from within the video player window in the Alarm Monitoring application. (Video events are typically created automatically by the system based on an event from an external device. A user generated event allows users to generate an event that is not tied to any device.)

Alarm	Event	Event Type	Description
Value Added	Value Added	POS	Event that indicates value added.
Video Event Threshold Reached	Video Event Threshold Reached	Video	Generated when the user-defined event threshold has been reached. (The percent of disk space used by video events has been reached, typically signaling the archive server to start archiving or purging.)
Video Server Disk Full	Video Server Disk Full	Video	Generated when the user-defined event threshold has been exceeded by 5% or more. (The percent of disk space used by video events has been exceeded by at least 5%, typically signaling the archive server to start archiving or purging.) If a user-defined event threshold has not been defined, this alarm/event will be generated when the video server disk space is 95% full of video events.
Video Server is Not Recording	Video Server is Not Recording	Video	Generated when it has been detected that the video recorder is no longer recording. A check is done periodically (default is every 10 minutes) to check to make sure that video is still being recorded. This event is generated when the check fails.
Void or Error Correction	Void or Error Correction	POS	Transaction that indicates a void or error correction
Walk Test ##	Walk Test ##	Fire	Generated when walk test ## is initiated. A walk test is used to test devices in the system and report devices addressed incorrectly. The device and the first zone programmed for this device are reported with each message.
Walk Test Uninstall	Walk Test Uninstall	Fire	Generated when the reported device was part of a walk test and has been physically disconnected from the system.
Walk Test Unprogrammed	Walk Test Unprogrammed	Fire	Generated when the reported device was part of a walk test and has been removed from the system (it is not longer configured in the system).
Walk Test Untest	Walk Test Untest	Fire	Generated when the reported device is no longer being tested (part of a walk test).

Appendix C: Reports

Reports are installed when Database Setup is run. All reports are installed on the database server under the ReportTemplates subdirectory in the B.A.S.I.S. installation path. By default, this location is **C:\Program Files\B.A.S.I.S.\ReportTemplates**. For more information, refer to The Database Setup Program appendix in the Installation & Setup User Guide.

Note: Refer to the release notes for the versions of Seagate Crystal Reports that are supported. The release notes are located on the root of the B.A.S.I.S. CD in a file named **B.A.S.I.S. ET release notes.rtf**.

Report name	Description
Access Denials and Grants, by Reader	Access Denied and Granted Events, grouped by Reader
Access Denials, Grants and Other Badge Events	All badge-related events, including time, reader, badge and cardholder name.
Access Denied Events	All Access Denied events, including time, reader, badge and cardholder name.
Access Denied Events, by Reader	Access Denied Events, grouped by reader.
Access Granted Events	All Access Granted events, including time, reader, badge and cardholder name.
Access Granted Events, by Reader	Access Granted events, grouped by Reader
Access Groups	Lists all Access Groups and the Access Levels contained in each group.
Access Groups With Levels	Access Group definitions including access level details.
Access Level Assignments to Cardholders	Listing of each Access Level, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded.
Access Level Assignments to Cardholders By Segment	Listing of each Access Level by Segment, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded to each segment. This report is valid only for systems that use the Segmentation feature.
Access Levels	Access Level definitions.
Access Panels	Access Panel definitions.
Active Visits by Cardholder Name	Listing of each active visit, grouped by cardholder name.
Active Visits by Visitor Name	Listing of each active visit, grouped by visitor name.

Report name	Description
Alarm Acknowledgments	All alarm acknowledgments, including the alarm information and acknowledgment notes.
Alarm Acknowledgments, by Definition	All alarm acknowledgments, grouped by alarm definition.
Alarm Acknowledgments, by Operator	All alarm acknowledgments, grouped by system operator.
Alarm Acknowledgments, by Panel	All alarm acknowledgments, grouped by panel.
Alarm Configuration	Alarm configuration summary.
Alarm Input Events	All Alarm Input events by date.
Alarm Panel Inputs	Definition of all Alarm Panel Inputs, grouped by Access Panel and Alarm Panel.
Alarm Panel Local Linkage	Lists alarm input/output local links on alarm panels.
Alarm Panel Outputs	Definitions of Alarm Panel Outputs, grouped by Access Panel and Alarm Panel.
Alarm Panels	Definition of all Alarm Panels, grouped by Access Panel.
All Events Over Time	A listing of all event types over time.
Anti-Passback Events	All anti-passback events over time.
Area Anti-Passback Configuration	Lists all anti-passback areas, including the reader entrances and exits.
Area Entrance History	History of all cardholders entering anti-passback areas, sorted by area and date.
Asset Classes	Listing of each asset class.
Asset Events	Listing of each asset event.
Asset Groups	Listing of each asset group.
Asset Types	Listing of each asset type.
Assets by Scan ID	Listing of each asset, grouped by Scan ID.
Assets by Type	Listing of each asset, grouped by type.
Assigned Assets by Cardholder	Listing of each asset, grouped by cardholder.
Assigned Assets by Scan ID	Listing of each assigned asset, grouped by Scan ID.
Assigned Assets by Type, Scan ID	Listing of each assigned asset, grouped by type and Scan ID.

Report name	Description
Audio Notifications and Instructions	Lists all audio notifications and instructions in the database.
Badge Type Configuration	Lists all badge types that have been configured in the system.
badges by Deactivate Date	Listing of all badges by deactivate date. Can be used to determine which badges are about to expire.
Badges Without Access Levels	Lists those badges that don't have access level assignments.
Card Formats	Definitions of all Magnetic and Wiegand card formats in the system. This combined report replaces the Magnetic Card Formats and Wiegand Card Formats reports that were available with previous software releases.
Cardholder Access to Readers	Listing of each Reader and which cardholders have access to that reader. Includes the associated Access Level and Timezone.
Cardholder Exit/ Entry	Displays user-defined Exit/Entry on a per-cardholder basis. In order for this report to work, readers must be designated as a 'Time and Attendance' Entrance or Exit reader on the Readers/Controls page. This report is not an Area APB report.
Cardholder Guest Access to Readers	Listing of each Reader, and which cardholders have access to that reader. Includes the associated Access Level and Timezone.
Cardholder Photo Gallery	All cardholder photos, sorted by name.
Cardholder Time and Attendance	Pairs each in-time with an out-time for cardholders gaining entry to time and attendance readers.
Cardholders by Badge Type	All cardholders sorted by badge type, no access levels shown. **Note:** ONLY personnel with badges assigned will be included in this report!
Cardholders by Last Name	All cardholders sorted by last name, with badges but no access levels. **Note:** ONLY personnel with badges assigned will be included in this report!
Cardholders Located in Each APB Area, by Date	List of the cardholders located in each anti-passback area, sorted by area and date
Cardholders Located in Each APB Area, by Name	List of the cardholders located in each anti-passback area, sorted by area and cardholder name
Cardholders with Access, by Badge Type	List of any access and precision access levels the cardholders have, sorted by badge type. **Note:** ONLY personnel with active badges AND access levels will be included in this report!

Report name	Description
Cardholders with Access, by Last Name	List of any access and precision access levels the cardholders have, sorted by last name. ONLY personnel with active badges AND access levels will be included in this report! **Note:** The **Cardholders with Access, by Badge Type** and **Cardholders with Access, by Last Name** reports replace the following reports from previous B.A.S.I.S. versions: • Cardholders With Access and Precision by Last Name • Cardholders With Access Levels, by Badge Type • Cardholders With Access Levels, by Last Name • Cardholders With Precision Access, by Last Name
CCTV Instructions	Summary of all CCTV instructions in the database.
Cisco AIC Inputs	Lists all Cisco AIC Inputs by panel.
Cisco AIC Outputs	Lists all Cisco AIC Outputs by panel.
Continuous Video	Lists all of the times that there has been continuous video archived.
Current Visits	Lists all currently signed in visits.
Destination Assurance Configuration	Lists all entrance readers, their settings and the associated exit readers.
Destination Assurance Exempt Cardholders	Lists all cardholders who has a badge that is exempt from destination assurance.
Device Status Events	Status events for all devices.
Dialup Events by Panel	Lists all dialup events by panel.
Dialup Last Connect Time	Lists the dialup last connect times.
Elevator Access Denied and Granted Events	All Access Denied and Granted events, including time, reader, badge, cardholder name and the floor to which access was attempted. All access denials and grants will be shown.
Emergency Events	All emergency events over time.
Enterprise Servers	Listing of Enterprise servers defined on this system. This report is valid only for systems that use the Enterprise Management feature.
Event Codes	Event code templates and event code mapping configuration.
Event Count By Panel	Listing of each event counts, grouped by panel.
Fire Device Input/ Outputs	Lists all fire input/outputs grouped by panel and fire device.
Global APB/ MobileVerify Occupancy, By Date	Shows the last known area accessed by each cardholder, sorted by date and time.

Report name	Description
Global APB/ MobileVerify Occupancy, By Name	Shows the last known area accessed by each cardholder, sorted by name.
Global I/O Linkages	Lists all of the global I/O linkages, including the input events and output actions.
Guard Tour Configuration	Lists all of the configured guard tours including checkpoints, actions and messages.
Guard Tour History	Lists all of the events, associated with checkpoints, that happened for each guard tour.
Hardware Panels	Listing of all hardware panels.
Holidays	List of all system holiday definitions.
Intercom Functions	Listing of all intercom functions.
Intercom Stations	Listing of all intercom stations.
Intrusion Detection Areas	Lists all intrusion areas grouped by panel.
Intrusion Detection Devices	Lists all of the intrusion detection devices grouped by panel.
Intrusion Panel User Groups	Lists all panel users grouped by panel user groups.
Last Location of Cardholders	Shows the last reader accessed by each cardholder, sorted by cardholder name.
Maps	List of available maps in the database.
MobileVerify User Transaction Log	Chronological log of all transactions performed.
MobileVerify User Transaction Log, By Operation	Chronological log of all transactions performed, grouped by operation.
MobileVerify User Transaction Log, By User ID	Chronological log of all transactions performed, grouped by User ID.
Monitor Stations	Shows all alarm monitoring stations defined in the system, including which monitor zones and access panels they are monitoring.
Monitor Zones	Monitoring Zone definitions.
Overdue Visits	Lists all scheduled visits that have not signed in.
Overstayed Visits	Lists all visitors logged into the facility, but whose badge or visit has expired.
Personal Safety Transmitter Assignments	Listing of all personal safety transmitter assignments.
Personal Safety Transmitters	Listing of all personal safety transmitters.

Report name	Description
Personnel in the Database	List of all personnel in the database, with basic information only.
Personnel Without an Active Badge	All personnel in the database which do not have an active badge assigned to them.
Personnel, Organization Details	List of all personnel in the database, with organization details. This report is designed for the standard cardholder layout. It may not work with user-customized cardholder layouts.
Personnel, Personal Details	List of all personnel in the database, with personal details. This report is designed for the standard cardholder layout. It may not work with user-customized cardholder layouts.
Point of Sale Registers	Lists all point of sale registers by point of sale device.
Precision Access Groups	Precision Access Group definitions.
Reader Assignments to Cardholders	Lists all cardholders that have access to a particular reader.
Reader Status Events	All reader status events, grouped by reader.
Reader Timezone Schedules	Reader timezone scheduling for reader modes.
Readers	Reader definitions, grouped by Access Panel.
Receiver Account Areas	Lists all receiver account areas, grouped by receiver account.
Receiver Account Groups	Lists all receiver account groups and the receiver accounts contained in each group.
Receiver Account Zones	Lists all receiver account zones, grouped by receiver account.
Receiver Accounts	Lists all receiver accounts.
Receiver Accounts that Failed to Report	Lists all of the receiver accounts that failed to report during their duration.
Receiver and Receiver Account Events	All the events that occurred on a receiver or receiver account.
Segment Badge Download Summary	For each segment, lists the count of badges that must be downloaded to the access panels in that segment. This report is valid only for systems that use the Segmentation feature.
Segments	Listing of segments defined on the system and their options. This report is valid only for systems that use the Segmentation feature.
SNMP Agents	Lists all SNMP agents sorted by segment and name.
SNMP Management Information Base Configuration	Lists all MIB data grouped by enterprise.
Text Instructions	All text instructions.
Timezones	Timezone definitions.

Report name	Description
User Permissions	All system users and their permissions.
User Transaction Log	Chronological log of all transactions performed on the system by users.
User Transaction Log, By User ID	Chronological log of all transactions performed, grouped by User ID.
Video Camera Device Links	Listing of all video camera device links.
Video Cameras	Listing of all video cameras.
Video Events	Listing of all video events.
Video Servers	Listing of all video servers.
Visit History	Listing of each visit.
Visitors	Listing of all visitors.
Windows Event Log Errors	All errors logged by the system to the Windows event log.

Index

A

Access Levels form (Cardholders folder)
- field table ... 163
- modify mode ... 163
- procedures ... 164
- view mode ... 163

Accounts ... 24
Acknowledge an alarm ... 120
Action Group Properties window ... 335
- field table ... 336
- procedures ... 336

Action History/Guard Tour Event Purging Properties window ... 337
- field table ... 337
- procedures ... 338

Actions ... 333
- procedures ... 333

Activate single or double left-click mode ... 110
Active visits ... 201
Add
- action ... 319
- action group ... 336
- action history/guard tour event purging action. 338
- action using scheduler right-click menu ... 327
- archive/purge database action ... 340
- asset ... 282
- asset groups and classes ... 289
- asset type/subtype ... 285
- automatic guard tour action ... 343
- badge record ... 157
- cardholder record ... 145
- columns ... 58
- deactivate badge action ... 349
- device output action ... 351
- device output group action ... 354
- execute function list action ... 356
- global APB system/segment reset action ... 358
- ISC database download action ... 360
- ISC firmware download action ... 362
- mask/unmask alarm input action ... 364
- mask/unmask alarm input for group action 366
- mask/unmask alarm mask group action ... 368
- mask/unmask door action ... 370
- mask/unmask door forced open action ... 372
- mask/unmask door forced open for reader group action ... 374
- mask/unmask door held open action ... 376
- mask/unmask door held open for reader group action ... 378
- pulse open door action ... 380
- pulse open door group action ... 382
- reader mode action ... 384
- reader mode group action ... 387
- readers ... 100
- report ... 240
- report print action ... 390
- reset use limit action ... 394
- sign out visitor action ... 396
- visit record ... 203
- visitor record ... 148

Add Action Wizard ... 333
Add Recipient window ... 220
- field table ... 220

Alarm
- descriptions ... 397
- icons ... 113
- overview ... 46
- pending alarms ... 114

Alarm Acknowledgment window ... 118
- functions ... 117

Alarm mask groups ... 51
Alarm Monitoring overview ... 21
Alarm Panel Reports form ... 248
- field table ... 249
- overview ... 248
- procedures ... 252

Anti-Passback Reports form ... 253
- field table ... 254
- overview ... 253
- procedures ... 257

Archive/Purge Database Properties window ... 339
- field table ... 340
- procedures ... 340

Arrange columns ... 58
Asset Classes form
- field table ... 287
- modify mode ... 286
- procedures ... 288
- view mode ... 286

Asset menu ... 45
Assets form (Assets folder) ... 280
- field table ... 280
- procedures ... 282

Assets form (Cardholders folder) ... 179
- field table ... 179
- procedures ... 179

Assign
- access levels to a badge ... 164
- access levels to cardholder group ... 168

activation/deactivation dates to access levels ... 166
asset to a cardholder ... 179
cardholder to an asset ... 292
classes to an asset ... 288
guard tour security clearance levels to a cardholder ... 184
precision access groups to a badge ... 172
Assignments form ... 290
field table ... 290
procedures ... 292
Automatic Guard Tour
respond to ... 314
schedule ... 313
Automatic Guard Tour Properties window ... 342
field table ... 343
procedures ... 343

B

Badge form
field table ... 153
modify mode ... 153
procedures ... 157
view mode ... 153
Badge Print Preview window
field table ... 187
procedures ... 188
Barcodes
CAC ... 138
scanning with a wedge scanner ... 138
Biometrics form (Cardholders folder) ... 173
field table ... 173
procedures ... 174

C

CAC barcodes ... 138
Cameras (surveillance-only) ... 90
Capture an image ... 92
Carcodes
configuring to read CAC barcodes ... 138
Cardholder form ... 144
field table ... 145
overview ... 144
procedures ... 145
Cardholder menu ... 43
Cardholder menu - bulk sub-menu ... 44
Cardholder search capabilities ... 133
Cardholders folder
field table ... 130
overview ... 129
procedures ... 133
Change cardholders folder view options ... 136
Change Network Video Password Properties window ... 345
field table ... 345
procedures ... 346
Checkpoint status and events diagram ... 316
Checkpoint time ... 309
Checkpoints ... 309
Comparison operators ... 133, 199
Configure
wedge scanner ... 143
Configure menu ... 37
Control menu ... 38
Control menu - “current device” sub-menu ... 38
Conventions used in this documentation ... 21
Create a video event ... 93

D

Date/Time Reports form ... 258
field table ... 259
overview ... 258
procedures ... 262
Deactivate Badge Properties window ... 348
field table ... 348
procedures ... 349
Delete
access levels assignments ... 170
alarm ... 121
alarm in Video Verification window ... 101
alarms (all) ... 122
asset ... 283
badge record ... 162
cardholder record ... 146
report ... 241
scheduled action using the scheduler right-click menu ... 329
selected group of cardholder records ... 146
visit record ... 208
visitor record ... 149
Deny or grant access ... 104
Destroy all cardholder data ... 147
Details form ... 217
field table ... 217
overview ... 217
Device group icons ... 64
Device Groups window ... 62
Device icons ... 65
Device Output Group Properties window ... 353
field table ... 354
procedures ... 354
Device Output Properties window ... 350
field table ... 351
procedures ... 351
Dialup panels - view last connection time ... 71
Directory Accounts form ... 181

field table 181
procedures 181
Disable strong password enforcement 23
Display
cardholder photo and live video 101
monitoring map 122
multiple hardware views 59
scheduler right-click menu 326
Display options - for users 55
Display Video Search window 95
Document organization 21
Double and single left-click mode 109
Download
database 72
firmware 72

E

Edit menu 34
E-mail form 218
Add Recipient window field table 220
field table 218
overview 218
Enable strong password enforcement 23
Encode badge configuration 161
Error messages 23
Event descriptions 397
Event Reports form 264
field table 265
overview 264
procedures 268
Event settings 87
Events diagram 316
Execute a command in single or double left-click mode 111
Execute Function List Properties window 355
field table 356
procedures 356
Exit the application 31
Export video to a file 92

F

Fast/group acknowledge feature 120
File menu 34
Filter report view 241
Filter search results 98
Find a cardholder or visitor associated with a visit . 203
Finished visits 201
First card unlock 384, 387
Functions - Alarm Acknowledgment window .. 117

G

Global APB System/Segment Reset Properties window 357
field table 358
procedures 358
Grant / Deny pop-up window 103
field table 104
Procedures 104
Grant or deny access 104
Guard Tour
launch a tour 309
respond 314
schedule automatic 313
Guard tour
tour events 311
Guard Tour Live Tracking window 311
Guard Tours form 183
field table 183
procedures 184

H

Hardware
tree view 60
update status of 70
Hardware view options 60
Help menu 43
How this document is organized 21

I

Icons
alarm 113
hardware device icons 65
hardware status icons 67
Images capture 92
ISC Database Download Properties window 358
field table 360
procedures 360
ISC Firmware Download Properties window ... 361
field table 362
procedures 362

K

Keyboard Wedge Settings window 137

L

Late event 309
Launch 88
Guard Tour 309
Launch video from camera 88
Left-click mode 109
Link
cardholder to a directory account 181
Linked maps 123
List options 50

Load a video file 89
Locate a device 71
Logging in
using automatic single sign-on 28
using manual single sign-on 29
without using single sign-on..... 25
Logging out of the application..... 31
Lookup a cardholder assigned to an asset..... 292

M

Maps
display..... 122
linked 123
Mask/Unmask Alarm Input for Group Properties
window 365
field table 366
procedures..... 366
Mask/Unmask Alarm Input Properties window 363
field table 364
procedures..... 364
Mask/Unmask Alarm Mask Group Properties
window 367
field table 368
procedures..... 368
Mask/Unmask Door Forced Open for Reader Group
Properties window 373
field table 374
procedures..... 374
Mask/Unmask Door Forced Open Properties
window 371
field table 372
procedures..... 372
Mask/Unmask Door Held Open for Reader Group
Properties window 377
field table 378
procedures..... 378
Mask/Unmask Door Held Open Properties window
375
field table 376
procedures..... 376
Mask/Unmask Door Properties window..... 369
field table 370
procedures..... 370
Menus..... 33
asset menu 45
cardholder menu
bulk sub-menu 44
cardholder menu 43
configure menu 37
control menu 38
current device sub-menu..... 38
edit menu 34
file menu 34
help 43
options menu..... 40
trace menu..... 36
view menu..... 34
window 43
Modify
access levels assignments 170
asset 283
asset classes assignment 288
asset group 180
badge record 159
badges for selected cardholder group 160
cardholder record..... 146
cardholder's permission to have visitors ... 177
cardholder's segment assignment..... 151
group of cardholder's segments..... 151
report..... 240
scheduled action using the scheduler right-click
menu 329
visit record 208
visitor record..... 149
Monitor (trace)
individual devices 77
Monitor video
in matrix view..... 89
with multiple cameras (successively)..... 90
with one specific camera 90
Multiple hardware views - display..... 59

O

Options - right-click..... 105
Options menu..... 40
Overdue event..... 309

P

Pan, tilt, and zoom 93
Password
enable/disable strong password enforcement ...
23
overview 22
standards 22
weak database warning..... 24
Pending alarms..... 114
Perform a device test..... 70
Performance requirements video search 88
Precision Access form (Cardholders folder)..... 171
field table 171
procedures..... 172
Precision access mode 50
Pre-configured acknowledgment notes - using. 120
Preview a badge 188
Preview and print a report..... 241
Print

badge ... 188
badge for a visitor ... 209
report ... 241, 299
Print Badge(s) window ... 198
field table ... 198
Print Report Options window ... 298
field table ... 299
PTZ ... 93
Pulse Open Door Group Properties window ... 381
field table ... 382
procedures ... 382
Pulse Open Door Properties window ... 379
field table ... 380
procedures ... 380

R

Reader Mode Group Properties window ... 386
field table ... 387
procedures ... 387
Reader Mode Properties window ... 383
field table ... 384
procedures ... 384
Reader Reports form ... 242
field table ... 243
overview ... 242
procedures ... 246
Rearrange alarms ... 115
Receiver Account Zone Reports form ... 274
field table ... 270, 275
overview ... 269, 274
procedures ... 278
Refresh
all actions ... 329
an action ... 328
Remove
access levels from a selected group of cardholders ... 170
columns ... 58
precision access groups from a badge ... 172
readers ... 100
Report Configuration form ... 236
field table ... 236
procedures ... 240
Report Print Preview window ... 304
field table ... 305
procedures ... 306
Report Print Properties window ... 389
field table ... 390
procedures ... 390
Report View Filter window ... 236
Reports ... 415
run a cardholder report ... 185
run a date/time report ... 262
run a reader report ... 246
run a receiver account zone report ... 278
run a visit report from the Visits folder ... 221
run an alarm panel report ... 252
run an anti-passback report ... 257
run an asset report ... 295
run an event report ... 268, 273
Reports form ... 221
field table ... 221
overview ... 221
procedures ... 221
Reports form (Assets folder) ... 293
field table ... 293
procedures ... 295
Reports form (Cardholders folder) ... 185
field table ... 185
procedures ... 185
Request Print Action Flowchart ... 392
Reset Use Limit Properties window ... 393
field table ... 394
procedures ... 394
Respond to an automatic Guard Tour ... 314
Retrieve the most recent search results ... 284
Retrieve the most recent visit search results ... 203
Right-click options ... 105
Run
alarm panel report ... 252
anti-passback report ... 257
asset report ... 295
cardholder report ... 185
date/time report ... 262
event report ... 268, 273
reader report ... 246
receiver account zone report ... 278
visit report from the Visits folder ... 221

S

Scanning barcodes with a wedge scanner ... 138
Schedule
action ... 319
action using scheduler right-click menu ... 327
automatic Guard Tour action ... 313
one-time password change ... 346
recurring password change ... 347
visits ... 201
Scheduler folder ... 317
Scheduler form (Scheduler folder) ... 318
field table ... 319
procedures ... 319
Search
for a cardholder record ... 135
for a cardholder's biometric record ... 174
for a device ... 71

for all visits by a selected visitor 200
for all visits for a specific date or time 202
for all visits to a selected cardholder 199
for an asset record 284
for devices 71
for empty values 134
for scheduled, active, or finished visits 201
on multiple fields 134, 199
report for specific information 308
specific portions of a camera view 96
text fields for "contains" 134, 199
video 95
Security clearance levels 184
Segments form (Cardholders folder) 150
field table 150
overview 150
procedures 151
Select
column configuration 58
events to monitor 57
Select a device
in single or double left-click mode 110
Select Date(s) window 213
Select Host Wizard - Search form 224
field table 224
overview 224
Select Host Wizard - Select form 226
field table 226
overview 226
Select Import Source window 234
field table 234
Select Time Range window 214
Select Visitor Wizard - Add form 231
field table 231
overview 231
Select Visitor Wizard - Search form 227
field table 227
overview 227
Select Visitor Wizard - Select form 233
field table 233
overview 233
Select Visitor Wizard - Select or Add form 229
field table 229
overview 229
Send
e-mail 124
page 126
Set start and end date 91
Sign in a previously scheduled visit 209
Sign In Visit(s) window 196
field table 196
Sign out a visit 211
Sign Out Visitor Properties window 395
field table 396
procedures 396
Single and double left-click mode 109
Sort alarms 115
Start an action 327
Status bar - Alarm Monitoring window 46
Status Search form 215
field table 215
overview 215
Stop an action 327
Surveillance-only cameras 90
Switch between camera and monitor views 93
Switch camera views displayed in Video Player 93
Switch log on 30
System Hardware Options window 55
System Hardware window 61

T

Test a device 70
Toolbars 33
Trace Configuration window 75
Trace menu 36
Tree view 60

U

Unassign an asset 292
Unlink
directory account 182
Update hardware status 70
User-defined display options 55

V

Video monitoring procedures 88
Video Monitoring window 79
Video Player 80
Video search performance requirements 88
Video Search window 84
display 95
Video Verification window 99
display 99
View
action history 327
current status of an action 328
last connection time for dialup panels 71
linked maps 123
video files 89
video on any computer 88
video search results 98
video tour 91
View menu 34
Visit form 212
field table 212
overview 212
Select Date(s) window field table 213

Select Time Range window field table 214
Visit reports 221
Visit right-click menu 192
Visit search capabilities 199
Visit search results 203
Visitor
find a cardholder or visitor associated with a visit 203
print badge for a visitor 209
search for all visits by a selected visitor 200
Visitor form 147
field table 148
overview 147
procedures 148
Visits
active 201
add a visit record 203
delete a visit record 208
find a cardholder or visitor associated with a visit 203
finished 201
modify a visit record 208
retrieve the most recent visit search results 203
right-click menu 192
run a visit report from the Visits folder 221
search capabilities 199
search for active visits 201
search for all visits by a selected visitor 200
search for all visits for a specific date or time .. 202
search for all visits to a selected cardholder 199
search for finished visits 201
search for scheduled visits 201
sign in a previously scheduled visit 209
sign out a visit 211
Visits folder
field table 194
overview 191
Print Badge(s) window field table 198
procedures 198
Sign In Visit(s) window field table 196
Visits form (Cardholders folder)
field table 176
modify mode 176
procedures 177
view mode 176

W

Weak database password warning 24
Wedge scanner
add a badge 137
configure 143
scanning barcodes 138
search for a badge 137
Wedge Settings window 137
Window menu 43

P.O. Box 5044
Indianapolis, IN 46250
Phone: (317) 849-2250

B.A.S.I.S.® ET Third Edition Alarm Monitoring User Guide, product version 5.10.421
Item number E805, revision 105, February 2004

Content of this document copyright © 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003 & 2004 by Lenel Systems International, Inc. BadgeDesigner™, FormsDesigner™, and MapDesigner™, are trademarks used by Best Access Systems with permission from Lenel Systems International, Inc. Windows, Windows XP, Windows 2000 are trademarks and Microsoft is a registered trademark of Microsoft Corporation. Integral and FlashPoint are trademarks of Integral Technologies, Inc. Crystal Reports for Windows is a trademark of Crystal Computer Services, Inc. Oracle is a registered trademark of Oracle Corporation. Other product names mentioned in this User Guide may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of the authors.

The software described in this document is licensed to Best Access Systems by Lenel Systems International, Inc. Portions of this product were created using LEADTOOLS © 1991-2003, LEAD Technologies, Inc. ALL RIGHTS RESERVED. The software includes ImageStream® Graphic Filters. Copyright © 1991-2003 Inso Corporation. All rights reserved. ImageStream Graphic Filters and ImageStream are registered trademarks of Inso Corporation.